DoD Chief Information Officer

Annual Information Assurance Report

Fiscal Year 2000

Table of Contents

Letter from the CIO

Technology advances have long been the primary motivators for the development of new military strategies, tactics and operations. For example, with the advent of the airplane, strategies of the day had to be adjusted to take into account not only controlling the battlefield, but also the airspace above it. This strategic paradigm shift was the direct result of the advancement of a new technology into a new role. As with any new strategy, the introduction of the airplane resulted in the rapid development of defensive counter-strategies. The history of conflict has seen the repetition of similar scenarios up to the present day.

Today, more than ever, in an environment of fast-paced technological advances, it becomes of paramount importance to understand and apply new technological developments while not allowing an adversary to exploit the inherent weaknesses they contain. Much as they transformed the civilian sector, computers and the networks that they support have revolutionized the way that military operations are conducted. The efficiencies gained by the application of new technologies give our military tremendous advantages that affect the strategic, tactical, and administrative environments. The very nature of the technological infrastructure, however, creates weaknesses that can become serious liabilities.

In response to that danger, the Department of Defense (DoD) has developed an information assurance (IA) strategy, called Defense in Depth, which offers a multitiered solution to ensure the security of our military's computer networks. From an information assurance perspective the capabilities that we must defend can be viewed broadly in terms of four major elements: local computing environments or enclaves; enclave boundaries; networks that link enclaves; and supportive infrastructures. The overlapping nature of the areas of defense creates a strong and reliable defensive fortress around our network operations.

The DiD IA strategy lies at the core of the objectives of the Joint Chiefs of Staff (JCS) Joint Vision 2020 (JV 2020) doctrine, which aims at improving the processes and capabilities that our military need in order to succeed in what will be the ever more complex global environment of the year 2020. The ultimate goal of JV 2020 is Full Spectrum Dominance, which relies on dominant maneuvers, precision engagements, focused logistics, and full-dimensional protection. The cornerstones of Full Spectrum

Dominance are the concepts of information superiority and innovation, each with IA at its core. Without the ability to defend itself against intrusion and attack, no network will be able to assume its role as a motivator for Full Spectrum Dominance.

The many challenges ahead will evolve as new technologies are developed and applied. This report outlines the efforts made to establish a strong and effective information assurance environment for the Department of Defense's effective operations, a foundation for the Joint Vision 2020. The impressive accomplishments described in this report demonstrate the scope of resources and energy dedicated to this task. Yet despite the successes obtained and the awareness generated for IA, we have to keep in mind that there remains much to achieve as the JV 2020 concept and its IA subset are being refined and realized.

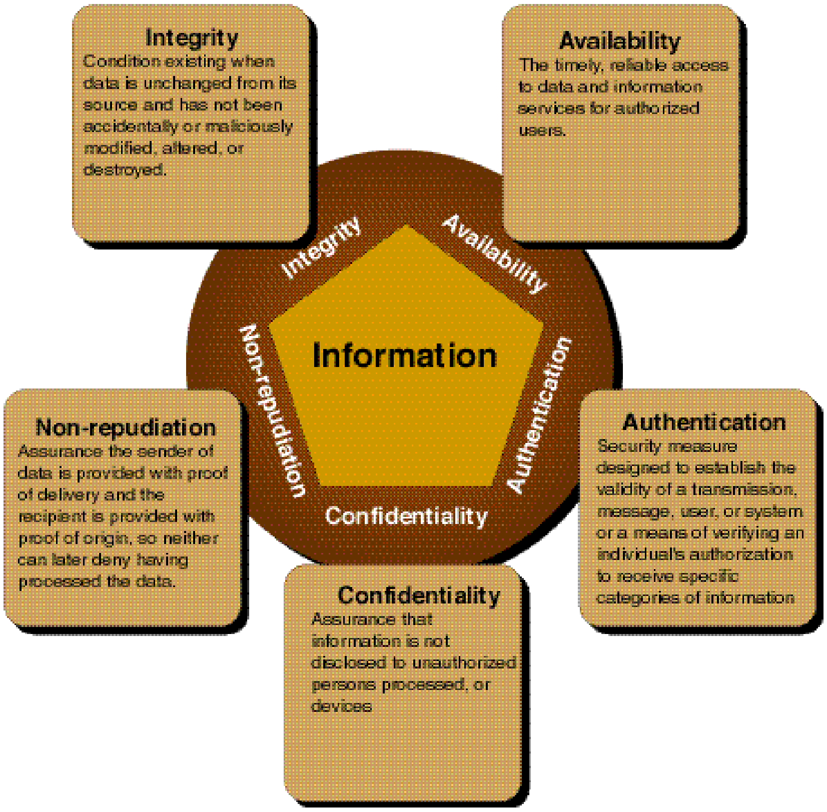
ALMoney

Arthur L. Money
DoD Chief Information Officer

Executive Summary

Introduction

The security of the United States depends on the ability of the Department of Defense (DoD) to protect its vital interests. To accomplish that mission, the DoD depends upon its information systems and networks to get the right information to the right people in the right place and at the right time. Yet, because of fast-paced technological advances and the interconnection and interdependence of these networks upon the commercial infrastructure— they are highly vulnerable and open to potential attacks. In such an environment, it becomes of paramount importance to understand and apply new technological developments in a way that does not allow an adversary to exploit the inherent weaknesses that they may contain. It is no surprise, therefore, that Information Assurance (IA), which provides the means to protect, detect and react to intrusions or attacks—whether internal or external—and to restore disrupted vital services as efficiently and



Integrity
Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

Availability
The timely, reliable access to data and information services for authorized users.

Non-repudiation
Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of origin, so neither can later deny having processed the data.

Authentication
Security measure designed to establish the validity of a transmission, message, user, or system or a means of verifying an individual's authorization to receive specific categories of information

Confidentiality
Assurance that information is not disclosed to unauthorized persons processed, or devices

effectively as possible, should emerge as a critical component of DoD operational readiness. Based on the five pillars of confidentiality, integrity, availability, non-repudiation and authentication, IA has been and is the focus of major efforts within the Department .

LEGISLATIVE MANDATES

For DoD, Information Assurance is defined as "Information Operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities." [DoD Directive S-3600.1, "Information Operations (IO)," 6 December 1996

Beyond the DoD's commitment to protect its systems and ensure that there is no disruption in its support of the warfighter, IA is an essential element in the implementation of security for the "increasingly vulnerable and interconnected infrastructure of the United States," as mandated by Presidential Directive 63 (PDD-63), dated 22 May 1998 entitled "Critical Infrastructure Protection.

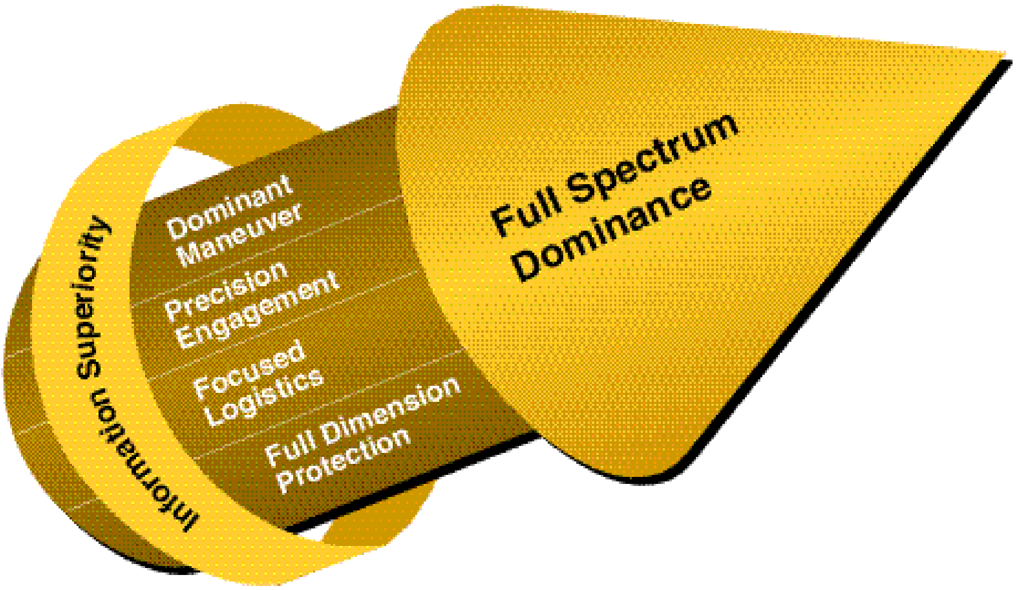
The Clinger-Cohen Act of 1996 (Public Law 104-106 , Division E Section 5123) assigned to the Department's Chief Information Officer (CIO) the responsibility to "ensure that the information security policies, procedures, and practices of the executive agency are adequate." Section 2224 of Title 10 of the United States Code (which was enacted in Section 1043 of Public Law 106-65, dated 5 October 1999) mandated that the DoD CIO present to Congress an Information Assurance Annual Report. The congressional language sets forth the following specific requirements: "Each year, at or about the time the President submits the annual budget for the next fiscal year pursuant to section 1105 of title 31, the Secretary shall submit to Congress a report on the Defense Information Assurance Program."

The initial version of the CIO Annual Report, published in 1999, covered IA topics related to regulatory, policy, organizational, technical, and threat issues. The February 2000 version of the report added depth, providing more detailed information on specific IA organizations, activities, and goals. This edition, unlike its calendar year predecessors, covers the fiscal year (FY) and provides information of greater scope on new and expanding IA initiatives and efforts. The introduction of a new format and the incorporation of color graphics and pictures further enhance this publication.

The FY 2000 IA Annual Report presents to Congress and to the IA community at large an overview of the status of Information Assurance in the DoD for Fiscal Year 2000. After describing the progress made in reaching the objectives of the program, it offers a summary of the program strategy and of changes in that strategy, and details the IA activities of the Office of the Secretary of Defense, Joint Staff, unified commands, Defense Agencies, Military Departments, and other supporting activities of the Department of Defense.

Why Information Assurance?

IA is a key component of Information Superiority, the ability to collect, process, and disseminate an uninterrupted flow of information, while exploiting or denying an adversary's ability to do the same. The continued development and proliferation of information technologies will substantially change the conduct of military operations, making information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control – Joint Vision 2020 (JV2020).



The IA Defense in Depth (DiD) strategy is central to the objectives of JV 2020, which is aimed toward improving the processes and capabilities that our military needs to succeed in what will be the ever more complex global environment of the year 2020. The ultimate goal of JV 2020 is Full Spectrum Dominance, which relies on dominant maneuvers, precision engagements, focused logistics, and full-dimensional protection. Full Spectrum Dominance relies on the concepts of Information Superiority and Innovation, each with IA at its core.

Thousands of unauthorized attempts are made daily to intrude into the sensitive computer systems that control key government and industry networks: defense facilities, power grids, banks, government agencies, and telephone and transportation systems. According to recent statistics, the Department of Defense alone was the target of more than 20,000 electronic attacks on its computer systems in 1999 and about 14,000 in the first seven months of Calendar Year 2000.

The DoD's information assurance challenge is enormous. The Department has about 1.5 million desktop computers. The number of computer systems reaches approximately 10,000, about 2,000 of which are mission-critical, meaning that they must be operational if the DoD is to successfully execute its myriad missions. These systems are prime targets to anyone trying to distract or prevent the Department from its mission. Unfortunately, the range of threats and vulnerabilities that the DoD must protect against include intentional (the script-kiddie to the state sponsored activity) and unintentional (errors, mistakes, omissions) human threats as well as environmental (both man-made and natural). Viruses and hacker attacks may be only a temporary annoyance, but the combination of these with other activities could seriously impair the Department's business processes and ability to execute its mission. In a resource constrained environment, conscious decisions must be made about where scarce resources should be spent to manage the risk to the DoD across the board. This risk management approach requires a clear understanding, not only of the threats and vulnerabilities, but the impact of tradeoffs among solutions. The balance of investment made in the three areas of focus - people, operations and technology - allows the DoD to get the "best bang for the buck" and leverage commercial investments in similar areas.

ADVANCES AND ACHIEVEMENTS

FY 2000 has seen significantly heightened IA achievements. Under the DiD umbrella, the wide range of IA-related programs and actions include education, training and awareness activities; research, development, and application of technologies such as biometric access control mechanisms; firewalls, intrusion detection systems, monitoring and management tools; applications, and operating systems. Strategic plans, policies and operational concepts are being developed to guide and direct IA efforts, while law enforcement and counterintelligence efforts focus on the identification and prosecution of cyberperpetrators. Readiness metrics and associated critical success indicators create a basis for measuring progress, red teaming exercises help prepare for diverse scenarios, and teams come together to react to ongoing cyberthreats. New policies are being developed to keep pace with the management challenges that accompany the introduction of new technology—and new threats.

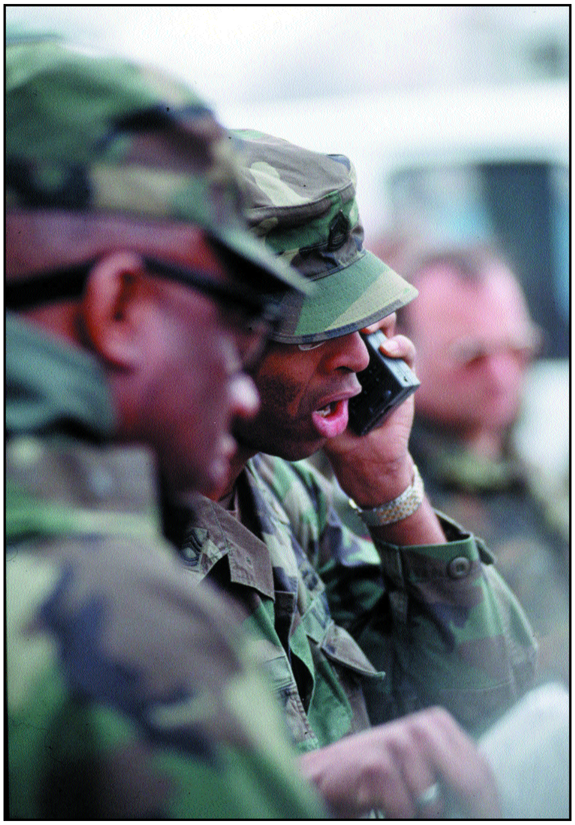
The present report comprehensively describes IA initiatives pursued by DoD during FY 2000. The C/S/A sections of the report detail specific projects and implementations. Key initiatives discussed fall in the areas of policy development and strategic planning, Public Key Infrastructure and Public Key Enabling, acquisition, research and development, and technical analyses and audits. Personnel-related issues presented include the IA education, training & certification, and awareness activities education; and the recruitment and retention of critical personnel.

The DoD IA arena has seen impressive accomplishments during FY 2000. New IA threats as well as vulnerabilities, however, emerge constantly in this global, networked environment and must be confronted. Besides presenting the objectives met during FY 2000, this report draws a roadmap that will help guide the Department toward success in facing the formidable challenges of the future and achieving the goals of Joint Vision 2020.

Introduction

TODAY'S CHALLENGES

The ever-widening expansion of systems and networks creates a new dimension for warfare that does not rely on tanks and battlefields but instead relies on computers and information infrastructures. The adversary can be anyone—a lone hacker, simply out for a thrill or bearing a grudge against the government; a member of a state-supported cyberwarfare group; or a cyberterrorist motivated by ideology, religion, or money. The new warfighter will have to be a cyberwarrior with nontraditional technical skills, rather than a traditional platform-based individual who relies on a tank, ship, or aircraft. In this new dimension, the Department of Defense needs to change its defensive strategy from a risk-avoidance approach to a risk-management approach.



A soldier makes use of wireless communications in the field.

Information assurance has emerged as a critical component of DoD operational readiness, providing the means to detect, react, and restore vital services as efficiently and effectively as possible following intrusions or attacks—whether internal or external. This is how DoD defines "information assurance":

> *Information Operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. [DoD Directive S-3600.1, "Information Operations (IO)," December 6, 1996]*

Until recently, concern for the security of the information and information systems of DoD existed only within the national security community and involved mainly systems that contained classified information. As the Department networked its activities and automated many of its functions, the concern expanded to include not only classified information but also sensitive unclassified systems and information that were becoming increasingly critical to the ability of the Department to achieve its mission. Numerous Government Accounting Office (GAO) reports, DoD Inspector General reports, and DoD-sponsored studies—both internal and external—pointed out deficiencies and vulnerabilities in the protection of these systems and the information that they contained. Recent outside incidents such as "Moonlight Maze," the "Melissa" virus, and the "I LOVEYOU" virus have highlighted the vulnerability of many of our systems to attack or infiltration.

As the DoD began to address these vulnerabilities, the complexities of the associated issues became increasingly apparent, along with the need for solutions. Initial attempts provided only partial and unsatisfactory answers. As a result, the notion emerged that the only answer lay in a multipronged approach involving people, operations, and technology.

With the Year 2000 (Y2K) rollover now behind, IA has become one of DoD's highest priorities. DoD is increasingly dependent upon a commercially based global information environment over which it has little control, thereby increasing its exposure and vulnerability to a growing number of sophisticated internal and external threats. Today's Internet-linked information systems create a new dimension for warfare, making it possible for a single adversary gaining access to a single network connection to surreptitiously disrupt many systems and networks. Once inside a system, an adversary could exploit it, as well as all the attendant networked systems.

Global Information Grid

Modern warfighting is centered on networks. Without secure and nonsecure networks such as Secret Internet Protocol Router Network (SIPRNET) and Unclassified but Sensitive Internet Protocol Router Network (NIPRNET), forces cannot accomplish their missions. Because of its importance, the network itself becomes a weapon system that enables the application of kinetic forces by providing

- Targeting, threat, and electronic-order-of-battle information;
- Weather predictions;
- Weapons availability, fuel, spare parts, and other logistical support data;
- Dissemination of air tasking orders, mission reports, and other vital command and control data; and
- Health and morale support functions of deployed forces.

This network eases force protection concerns by allowing the deployment of necessary personnel only. Those personnel can reach back to rear echelons for critical support information.

Information systems and networks allow this to occur quickly, efficiently, and securely.   This weapons system network, referred to as the Global Information Grid (GIG), is truly global. The GIG, as defined by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD[C3I]), is a "globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers and support personnel."   The GIG not only serves the warfighter's need for Information Superiority (IS) but also addresses the critical concerns of frequency spectrum and information infrastructure management. The GIG is a constantly evolving entity as technologies, policies and capabilities are developed to take advantage of its vast potential.

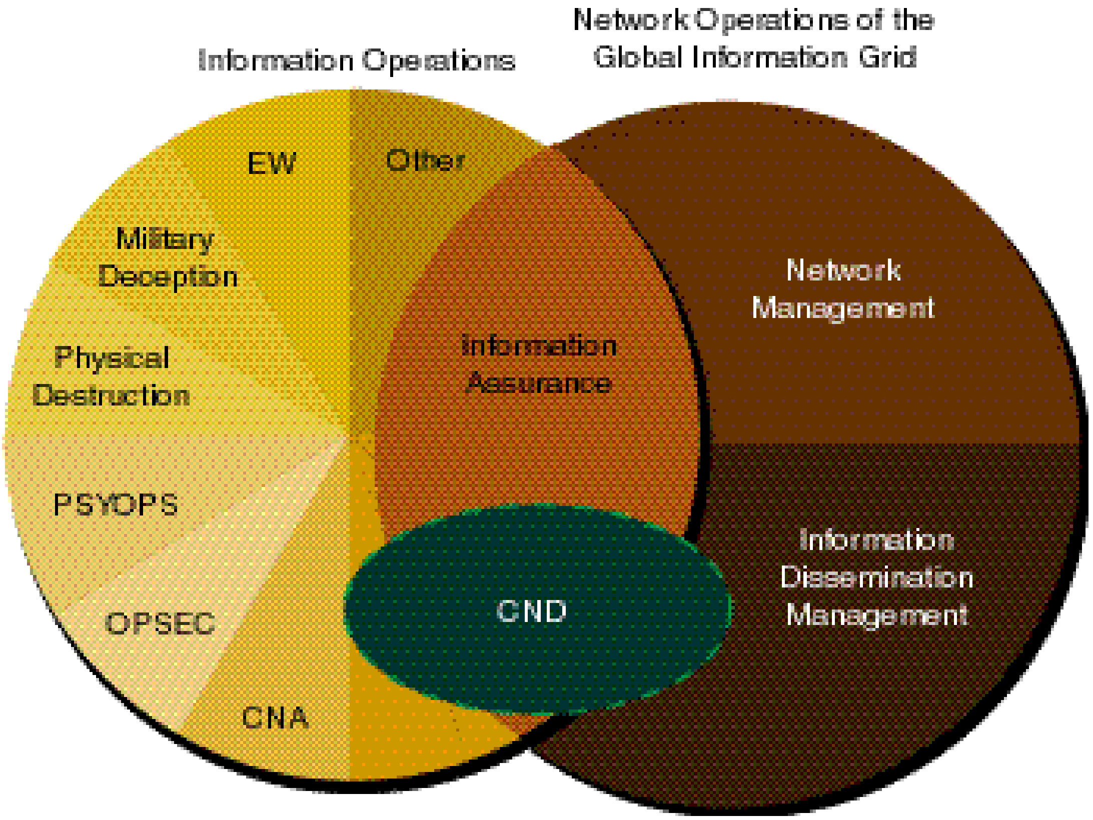


Figure 1. Information Operations and Network Operations of the Global Grid

In order to be truly operational, the GIG must provide end-to-end visibility, control, and support to manage and protect networks and the information they carry. To maintain the integral capabilities, the GIG must be scalable, as well as resourced and upgraded as required. In this context, the GIG can fully support combat operations from the initial sensor, to the decision maker, to the shooter, to battle damage assessment in near real-time. This capability gives the US forces a tremendous advantage in battlefield awareness and enables senior officers to make combat decisions based on near real-time intelligence.

The GIG is not just a combat tool, but also provides benefits and capabilities in the areas of logistics, computing services, communications, network operations and information management. Each of these areas perform specific and important functions that when fully integrated, enable the DoD to perform its mission more successfully, effectively and efficiently. Information Assurance, as defined by the Joint Staff, falls within the network operations area of the GIG. It has gained increasing importance as the crucial link in the implementation of the GIG concept due to its focus on maintaining the integrity of all of the data and information that is sent across the GIG, and thus, is a powerful tool. Figure 1 discusses IA's relationship with network operations and other facets of the GIG.

As can be seen in Fig 1, IA is part of Network Operations, Information Operations, Electronic Warfare, Military Deception, Physical Destruction, Psychological Operations, Operational Security, and Computer Network Attack and Defense. Also, as depicted in this figure, Computer Network Defense (CND) is nearly synonymous with IA and plays a large role in Network Operations. The same warfighters whose mission is IA are also experts in defending computer networks. In a world in which computers are ubiquitous and are, for the most part networked, the boundaries between these two mission areas are fast disappearing.

A CLOSER LOOK AT IA

In today's environment of sophisticated weaponry and rapid global force projection requirements, the ability to provide timely and accurate information is vital to all aspects of DoD operations. The capability of DoD to execute its mission from peacetime through conflict and back to peacetime depends greatly upon both the interconnected set of information systems and networks called the Defense Information Infrastructure (DII) and the expanding national and global infrastructure. As the means to counter cyberthreats, IA has emerged as a critical component of DoD's operational readiness. It enables the systems and networks of the DII to provide protected, continuous, and dependable service in support of both warfighting and business missions. Relying upon a risk-management blend of managerial, procedural, and technical activities, IA works at ensuring the availability, integrity, authenticity, confidentiality, and nonrepudiation of information services. It also provides the means to efficiently reconstitute these vital services following an attack. It focuses on DoD missions and infrastructure that are substantially interwoven with our National Information Infrastructure (NII) and increasingly dependent on services derived from the Global Information Infrastructure (GII). Information superiority is at the very foundation of our vision of modern warfare, and IA is essential to achieve and maintain this superiority. IA is an integral part of Joint Vision 2020 and the ability to integrate intelligence, command and control, and battlefield awareness functions into joint and combined operations. IA is also an essential element in implementing protection of critical national infrastructures as mandated by the Presidential Decision Directive 63, Critical Infrastructure Protection.

This view emphasizes the importance of IA to the Department's warfighting capability and the need to integrate IA into every facet of military operations. This integration goes beyond IA technology acquisition: it will require, throughout the Department, a heightened awareness of both the criticality of information operations and the role of IA in support of operational missions. Most important, full integration requires a clear operational understanding of the risks and impact on Defense missions of an inadequate IA. Achieving this perspective will require significantly changing the approach to IA across the Department and recognizing that IA is a warfighting concern, to be ranked appropriately in Departmental attention and in budgetary trade-offs with other warfighting capabilities. The purpose should be to attain increasingly effective, yet affordable, IA capabilities. That requires operational attention and a continuous assessment process of both risk and return on investment.

To ensure that the vision of information superiority is achieved, the Defense-wide IA Program includes a strategy and two specific goals to guide the Department's activities. The goals are to protect mission-critical information and to provide robust systems and reconstitution when required. An important factor in achieving these goals is the development and cultivation of a cadre of IA professionals.

The strategy needed to help achieve these goals is process-oriented and based on the principles of risk management, continuous improvement, and performance-based investment. It reflects the strong link between IA and operational readiness and the need for continuous monitoring and accurate reporting of the Department's IA posture. IA operations need a big picture viewpoint. The use of the DoD Chief Information Officer's (CIO's) organization and of management processes will help to ensure that the IA solutions applied are DoD-wide, not exclusive to one area of the Department. In addition, the DoD CIO must turn IA awareness into a key ingredient throughout the organization. All levels of DoD must be able to make the distinction between information that is operationally sensitive and information that can be made available to the public.

This approach must also address information infrastructure vulnerabilities—physical ones as well as those open to cyberattack. The disruption, failure, or destruction of equipment or services (e.g., power, cooling, and/or telecommunications) that support the information infrastructure can potentially disrupt critical services just as much as cyberintrusion. The Department's IA improvement efforts are guided by the objectives and strategies contained in the Information Management (IM) Strategic Plan.

The goals of IA are to protect and guarantee the legitimacy of electronic communications sent through the Internet and by other electronic means. The following terms describe the basic services that IA provides to information (e.g., a supply order for engine parts) sent between DoD users:

- Availability: Timely, reliable access to data and services for authorized users
- Identification and Authentication: The process used by the system to recognize an entity—a security measure designed to establish the validity of a transmission, message, or originator, or as a means of verifying with some degree of assurance an individual's authorization to receive specific categories of information
- Confidentiality: Assurance that information is not disclosed to unauthorized persons
- Integrity: Protection against unauthorized modification or destruction of information
- Nonrepudiation: Assurance that data are sent—with proof of delivery and the recipient being provided with proof of the sender's identity—so that neither can later deny having processed the data

Defense in Depth Strategy

Defense in Depth (DiD) is the strategy that the DoD is pursuing to ensure success in both cyberwarfare and other types of warfare that are dependent upon information superiority. Critical to the military's ability to conduct warfare, IA is the responsibility of all modern warfighters. Because of the universal nature of the global information grid, a risk assumed by anyone, at any level, is a risk assumed by all. IA is therefore necessary at all levels. That goal can be achieved through the concept of DiD, which employs mechanisms on successive layers at multiple locations. Through a structured and deliberate risk analysis process, leadership can make effective risk-management decisions on how to best deploy the appropriate DiD strategy. Figure 2 depicts the components of this strategy.

Personnel: People using technology to conduct operations form the central element of DiD. People design, build, install, operate, authorize, assess, evaluate, and maintain protective mechanisms.

Technology: To conduct an effective cyberdefense, DoD must have a well-stocked arsenal of technological weapons and the skills to use them. Because technology tools and products used in DoD IA solutions are evaluated under programs designed to ensure their functionality and utility, DoD can have greater confidence in their effectiveness.

Operations: IA policy drives IA operations by establishing goals, actions, procedures, and standards. IA policy formally states security requirements in terms of what must be done and what must not be done. Policy establishes standards that define uniform and common features and capabilities of security mechanisms, the metrics to measure the various dimensions of IA, and the desired or required level of attainment.

To prevent the potential breakdown of barriers and the invasion of the innermost (or most valuable) parts of a system, defenses must be constructed in successive layers and by setting safeguards at various locations. These different locations are expressed as the networks and infrastructures that link the enclaves, network enclave boundaries, local computing networks, and supporting infrastructure.

The network and infrastructure linking enclaves comprise large transport networks and other transmission and switching capabilities, including operational area networks, metropolitan area networks, campus area networks, and local area networks that extend coverage from broad communities to local

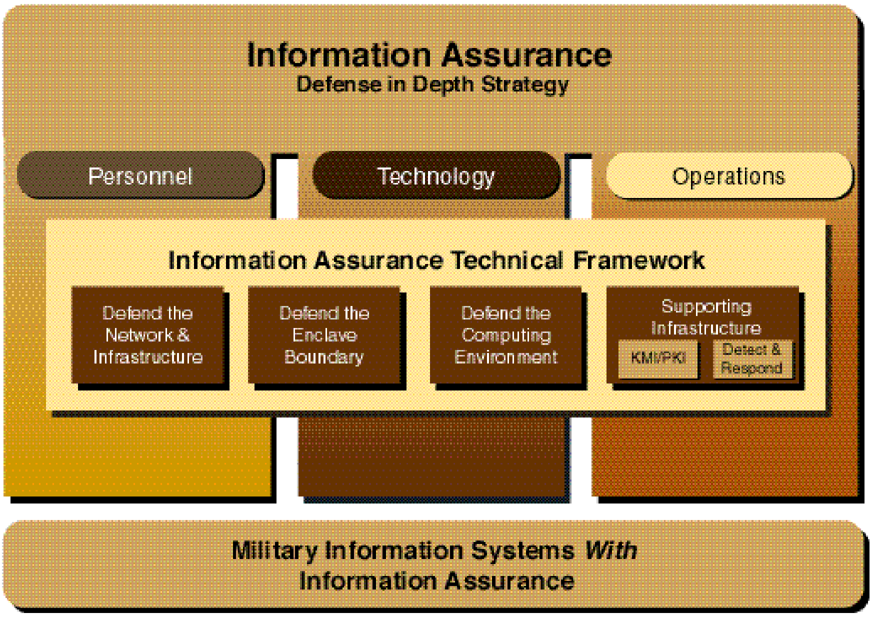

Information Assurance
Defense in Depth Strategy
Personnel
Technology
Operations
Information Assurance Technical Framework
Defend the Network & Infrastructure
Defend the Enclave Boundary
Defend the Computing Environment
Supporting Infrastructure
KMI/PKI
Detect & Respond
Military Information Systems *With* Information Assurance

Figure 2

bases. The target environment for networks and infrastructure includes data, voice, wireless (e.g., cellular, paging), and tactical networks that support both operational and strategic DoD missions. These networks can be DoD-owned and operated or provided through leased lines.

Tactics used to defend the network and infrastructures include the use of multiple and redundant data paths to allow more than one available alternative physical medium or route for data transport. This tactic counters the physical loss or damage of a transmission medium and a denial-of-service attack. The applicable technologies are monitoring and management tools, intrusion detection systems (IDSs), encryption of data, and antitamper mechanisms.

A network enclave boundary marks—with personnel and physical security measures—the perimeter of an environment, known as an enclave, that is under the control of a single authority and may control multiple networks. Enclaves may be logical, such as an operational area network, or they may be based on physical location and proximity. The enclave boundary exists at the point of connection for a LAN or similar network to the service layer. Would-be hackers can target at the enclave boundary many points such as the service layer networks (including modem connections), classified LANs within a classified WAN, remotely connected laptops, and high-to-low and low-to-high network classification transfers.

Technologies used to defend the enclave boundary include identification and authentication (I&A) tools, firewalls, virus detectors, IDSs, proxy servers, and monitoring and management tools. More specifically, I&A tools include user names and passwords, PINs, and biometric mechanisms that identify individuals based on their physical characteristics. There are many excellent and widely used firewall systems currently available. These can screen out traffic based on such criteria as sender or destination address and requested service or task. IDS, virus, and

Standing on guard in defense of the perimeter.

monitoring and management tools all provide the ability to filter traffic at the enclave boundary and determine whether it is unauthorized or malicious. Proxy servers can block end-user requests to access off-limits network addresses. This capability is useful when such sites are known sources of malicious code or other hostile actions.

Defense of the computing environment focuses on servers and clients, including installed applications, operating systems, and host-based monitoring capabilities. The computing environment also includes the end-user workstations, both desktop and laptop, including peripheral devices; servers, including web, applications, and file servers; applications such as intrusion detection, secure mail and web, and access control; and the operating system.

Many of the technologies that defend the computing environment and those used for the networks and enclave boundaries overlap. These include I&A tools, encryption, IDS, and monitoring and management systems. In addition, identities can be verified through digital signatures that function much like written signatures, but use complex algorithms as their verification mechanism. Vulnerability checkers are employed that scan the internal networks for vulnerabilities before they can cause harm. Backup technologies for saving and updating data stored on a server or workstation can serve as a contingency against a failed hard drive, malicious attack on a computer, etc., and minimize the risk of losing vital information. In case of a breach, it is vital to have the ability to restore and continue on with the mission in a timely manner.

Supporting infrastructures generally refer to two highly important components that provide crucial services enabling the first three defensive postures. The DoD is currently implementing a Key Management Infrastructure (KMI) and Public Key Infrastructure (PKI) that will enable secure communications with integrity, identification and authentication, confidentiality, and nonrepudiation services. KMI provides a common unified process for the secure creation, distribution, and management of the public key certificates and traditional symmetric keys that enable security service for the network, enclave, and computing environments. KMI/PKI manages the cryptographic keys for both symmetric and public key-based cryptography and also manages the certificates used by public key-based security services.

The second component is the detect-and-respond capability. The detection, reporting, and response infrastructure enables rapid detection of, and reaction to, intrusion and enables operational situation awareness and response in support of DoD missions. Local infrastructures support local operations and feed regional and DoD-wide infrastructures so that DoD can react quickly, regardless of the scale of the intrusion. The infrastructure for situation awareness and response cells includes incident responses that allow skilled specialists to assess suspicious activities and to judge whether assistance or response is needed. The United States Space Command (USSPACECOM) has overall authority for the Joint Task Force – Computer Network Defense (JTF-CND) and has led the development of the DoD's detect-and-respond capability. In addition to the JTF-CND and each major Service Component, almost every Commander in Chief (CINC) and Agency has created some form of computer emergency response team (CERT) that enables them to provide a detect-and-react capability that complements USSPACECOM's efforts.

SUMMARY

In light of its crucial importance for classified and unclassified network systems, IA remains one of the highest priorities for DoD.

Major progress has been made in the IA arena during fiscal year (FY) 2000. DoD has begun the transition from risk avoidance to risk management. Through application of the tenets of Defense in Depth and looking forward toward Joint Vision 2020, significant advances have been made in the areas of DoD Information Technology Security and Certification and Accreditation Process (DITSCAP) implementation; the introduction of new protective technologies, policies, and methodologies; IA and security awareness training; Human Resource management of IA resources; and PKI/Public Key Enabling (PKE).

IA challenges still remain. The major and ongoing one is for DoD to be able to keep pace with rapidly evolving technologies (both friendly and hostile) and network communication capabilities. Related to this challenge is the need to keep personnel current with the new technologies and understanding them enough to be able to defend against consequent security threats and initiatives. Near-term plans can address these challenges.

DoD is determined to continue down the road of progress in the IA arena, especially in the areas of technology, policy, and process development, until its IA vision becomes a reality.

DIAP Functional Areas

A CLOSER LOOK AT DIAP

The Defense-wide Information Assurance Program (DIAP) was established in 1998 by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (C3I). Its overarching mission is to ensure that the Department of Defense's vital information resources are secured and protected by unifying/integrating IA activities to achieve information superiority. DIAP achieves this by ensuring the protection and reliability of the Defense Information Infrastructure and providing a common management framework and the central oversight necessary for DoD information assurance. Through this common framework, DIAP can transform DoD IA efforts from a technical issue to an operational imperative and leverage its size and knowledge-sharing abilities to develop powerful, DoD-wide solutions.

The long-term vision for DIAP is that by 2005, it will be the model organization for implementation of enterprisewide IA. It will accomplish this by

- Institutionalizing IA in DoD mission areas and processes,
- Measuring and articulating improvements in the Department's IA posture,
- Identifying and justifying IA investments,
- Attaining value-added partner status within the IA community,
- Operationalizing IA to have situational awareness of the information environment,
- Being DoD's primary resource for IA issues and concerns, and
- Creating a national passion for IA.

For DIAP to focus on DoD-wide functional and programmatic issues, it is organized into two teams. The first is the Functional Evaluation and Integration Team (FEIT), which continuously evaluates DoD and Component IA programs to ensure that the Defensewide application of IA functions is consistent, integrated, efficient, and programmatically supported. The FEIT is divided into eight functional areas:

- Readiness Assessment
- Human Resources Development
- Policy Integration
- Security Management
- Operations Environment
- Architectural Standards and System Transformation
- Acquisition Support and Product Development
- Research and Technology

(In the next section of this report, each of these functional areas will be described in greater detail, along with their FY 2000 accomplishments.)

The second team is the Program Development and Integration Team (PDIT), which provides oversight, coordination, and integration of DoD IA resource programs. In performing this mission, the PDIT develops IA program categories and transforms IA resources into operational capabilities. It is also responsible for developing input to the Defense planning documents and for preparing the DIAP Congressional Justification Book (CJB). In its oversight role, PDIT monitors the IA plans, activities, and resource investments of Components and assesses the adequacy of the resources. In addition, it prepares and coordinates responses to IA program queries from Congress; the Under Secretary of Defense, Comptroller; and the Office of the Director, Program Analysis and Evaluation (PA&E). (Resource and program information is contained in the separate annex to this report.)

In addition to the FEIT and the PDIT, DIAP maintains many liaison positions that enable it to work more effectively with the various CINCs/Services/Agencies (C/S/A). These liaisons allow DIAP to address issues specifically related to a particular activity and to initiate, coordinate, and oversee IA activities. DIAP has liaison elements to the following communities:

- Law Enforcement and Counterintelligence
- Intelligence
- Critical Infrastructure Protection
- Joint Staff
- Reserve Component
- Services
- Agencies

The liaisons form a critical link between the functional and programmatic resource areas and the actual activities.

POLICY

FY 2000 was an ambitious year for formulation of DoD policy. Many policy memoranda were signed, and several DoD Directives and Instructions were developed and informally coordinated or formally staffed. As the fiscal year closed, the DIAP was continuing to press forward in the development of key policies required to ensure Departmentwide information assurance. Also, in order to facilitate greater access to the latest policy directives, the Policy On-Line Resource website began operation in August 2000.

The program involved developing a new policy framework and realigning as 8500-series publications new or updated information assurance (IA)-related DoD issuances. The new framework includes the following:

8500	General
8510	Certification and Accreditation
8520	Security Management [Security Management Infrastructure (SMI), Public Key Infrastructure (PKI), Key Management Infrastructure (KMI), and Electronic Key Management System (EKMS)]
8530	Computer Network Defense
8540	Interconnectivity/Multilevel Security
8550	Network/Web (Access, Content, and Privileges)
8560	Assessments [Vulnerability Analysis and Mitigation Program,Vulnerability Analysis and Assessment Process (VAAP), Red Team, and TEMPEST Testing]
8570	Education, Training, and Awareness
8580	Other
8590	Reserved

Significant individual policies directly related to IA are described below (these efforts are presented in the framework sequence):

Deputy Secretary of Defense Memorandum, "DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No8-8001, 'Global Information Grid,'" 31 Mach 2000. This Guidance and Policy Memorandum is the capstone document that defines the major policy principles and associated responsibilities for implementing the Global Information Grid (GIG). Specifically, this policy assigns management responsibilities for managing the GIG on an enterprise basis, in compliance with the Clinger-Cohen Act of 1996 and Title 10, U.S.C., Section 2223. It provides key policy principles for networks, computing, information assurance, information management, and network operations, including their interoperability.

Deputy Secretary of Defense Memorandum, "Department of Defense Chief Information Officer Guidance and Policy Memorandum

No. 6-8510, ‘Department of Defense Global Information Grid Information Assurance," 16 June 2000. This Guidance and Policy Memorandum for Global Information Grid (GIG) Information Assurance (IA) articulates policy and assigns responsibilities for secure, interoperable information capabilities that meet both warfighting and business needs for the DoD. It provides the framework for achieving IA by ensuring the availability of systems, the integrity and confidentiality of information, and the authentication and nonrepudiation of electronic transactions. It directs all DoD Components to follow a Defense in Depth strategy, which will provide protection to networks, enclaves, and computing environments while making appropriate use of supporting IA infrastructures (e.g., key management, public key certificates, and directories). The accompanying GIG IA Implementation Guidance provides details on the selection of the appropriate security countermeasures required to implement Defense in Depth in order to secure the GIG architecture.

The direction provided in this Memorandum and the Implementation Guidance discussed above are being formally incorporated into the **DoD Directives System by DoD Directive 8500.aa, "Information Assurance," and DoD Instruction 8500.bb, "Information Assurance Implementation.** " These issuances will serve as the capstone documents for IA across DoD. (They are currently in the informal coordination process, with publication expected in spring 2001.)

DoD Instruction 8510.aa, "Department of Defense InformationTechnology Security Certification and Accreditation Process (DITSCAP)" (draft).This Instruction is an update of DoD Instruction 5200.40, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)," 30 December 1997.

The DITSCAP provides a process for assessing the security posture of an individual system and determining how each system can affect the security posture of every other system in its computing environment. The update is essentially a refinement of the guidance provided in the current document. (It will be published in early 2001.)

DoD Manual 8510.1-M, "Department of Defense InformationTechnology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 2000. This Manual is a stand-alone reference. It provides detailed guidance on conducting the certification and accreditation process; it also includes descriptions of the activities and tasks associated with each phase of the DITSCAP, their relationship to the system life cycle, and a summary of management roles and responsibilities.

DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," 12August 2000.

Replacing Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," 6 May 1999, this Memorandum updates DoD policies for the development and implementation of a Departmentwide PKI.

The goal of this DoD-wide infrastructure is to provide general-purpose PKI services to a broad range of applications, at levels of assurance consistent with operational imperatives. The Department is taking an aggressive approach in acquiring and using a PKI that meets requirements for all IA services. This Policy Memorandum encourages widespread use of public key-enabled applications and provides specific guidelines for applying PKI services throughout the Department.

DoD Chief Information Officer Memorandum, "Public Key Enabling of Applications, Web Servers, and Networks for the Department of Defense (DoD)" (draft). DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," 12 August 2000, provides guidance as to which applications, such as e-mail and web browsers, must be public key-enabled and sets a schedule for accomplishing that task.

DoD Directive O-8530.aa, "Computer Netwok Defense (CND)" (draft). This Directive establishes the CND policy, definition, and responsibilities necessary to provide the essential structure and support to the U.S. Space Command for CND within DoD information systems and computer networks. CND encompasses actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks. (This Directive and the Instruction described below are currently in formal staffing, with publication expected in early 2001.)

DoD Instruction O-8530.bb, "Support to Computer Network Defense (CND)" (draft). This Instruction prescribes the detailed procedures necessary to implement DoD O-8530.aa.

DoD Instruction 8540.aa, "Interconnection and Data Transfer between Security Domains" (draft). This Instruction will establish DoD policy and procedures for the interconnection of information systems of different security domains, to include engineering, installation, certification, accreditation, and maintenance of such interconnections. (Publication is expected sometime in 2001.)

Assistant Secretary of Defense, Command, Control, Communications, and Intelligence [ASD(C3I)] Memorandum, "Policy Guidance for Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems," 7 November 2000. Mobile code technologies can be used maliciously to deny service, corrupt or expose sensitive information, and destroy data. To protect DoD systems from the risk posed by malicious mobile code, this Policy Memorandum defines risk-based technology categories and specifies conditions and restrictions on the use of mobile code technologies in each category. Uniform DoD-wide guidelines will foster the effective use of mobile code in the DoD, while enabling sound management of the posed risk.

Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Information Assurance Vulnerability Alert (IAVA)," 30 December 1999. To protect DoD networks against potential vulnerabilities, this Policy Memorandum directed that increased emphasis be placed on the Information Assurance Vulnerability Alert (IAVA) process. (IAVA was instituted in 1998 to provide positive control of vulnerability notification and corresponding corrective action within DoD.)

DoD Instruction 8560.cc, "Information Assurance Vulnerability Reporting and Mitigation" (draft). This Instruction will formalize a DoD Information Assurance Vulnerability Reporting and Mitigation program. The resultant effort will draw upon existing guidance for vulnerability reporting and provide additional guidance on the vulnerability notification processes, including specific guidance on the Information Assurance Vulnerability Alert (IAVA) process. (Publication is expected sometime in 2001.)

DoD Instruction 8560.aa, "DoD Telecommunications Monitoring" (draft). This Directive will update policies and responsibilities for the monitoring and testing of DoD telephones and networked computer systems, to include penetration testing (more commonly known as "red teaming").

Deputy Secretary Of Defense Memorandum, "Implementation Of The Recommendations Of The Information Assurance And Information Technology Integrated Process Team On Training, Certification, And Personnel Management In The Department Of Defense," 14 July 2000. This memorandum assigns action to implement the recommendations outlined in the final report of the Information Assurance (IA) and Information Technology (IT) Integrated Process Team (IPT) on training, certification, and personnel management in the department of defense. The IPT was tasked to examine issues pertaining to the hiring, retention, training, and certification of IA and IT professionals.

POLICY ON-LINE RESOURCE

The Information Assurance (IA) Policy On-line Resource (POLR) is a web-based information resource and portal for IA policy, procedures, and information. POLR, in its final form, is intended to be a comprehensive IA reference source that will simplify IA for a wide range of users by providing a single reference point for obtaining up-to-date materials. The first of three planned phases of POLR became operational in August 2000. The primary target audience includes DoD policy makers, Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), network security officers, security technicians, and program managers. POLR is also more generically aimed at Federal Department and Agency IA users, General Accounting Office (GAO) and DoD Inspector General (DoDIG) auditors, and Critical Infrastructure Assurance Office (CIAO) users.

POLR provides access to selected, IA related documents such as applicable public laws and other national policy and guidance documents, however, its emphasis is on DoD directives, instructions, regulations, handbooks, manuals, and other memoranda. In certain technical areas, POLR provides links to appropriate websites that will provide greater understanding or illumination of a certain topic (e.g. POLR links to the DISA website for greater certification and accreditation discussion).

POLR also provides links to a variety of other government sites where IA information may be available. Many are DoD sites, to include the Joint Staff and CINC/Service/Agency (C/S/A) IA/Information Systems Security (INFOSEC) pages, Network Operations Centers (NOCs), Computer Emergency Response Teams (CERTs), and law enforcement/computer network defense sites. Links are also provided to the Federal Register, National Security Council documents, the U.S. Security Policy Board, CIO Council, Office of Management and Budget, Government Accounting Office, National Institute of Standards and Technology, etc. Additional links will be added, as appropriate, based on user requirements and feedback

While Phase 1 is currently operational, Phase 2 is planned to provide an expanded search capability; document snapshots, relationships, and genealogy; full text and keyword searches; executive summaries where appropriate; and IA and IA-related reports, studies, white papers. Phase 3, also in the planning stage, will focus on classified documents and information (available to SIPRNet users). POLR is located at http://www.c3i.osd.mil/org/sio/ia/diap2/.

Newly arrived Marines are led through an encampment near an airfield during Operation Desert Shield.

HUMAN RESOURCES

The Human Resources Development Functional Area was established to develop and institutionalize the means for continuous improvements in the Education, Training and Awareness (ETA) of DoD personnel and Manpower resources required to carry out the Department's IA mission. Significant activity has occurred throughout the Department of Defense and in the Federal government impacting this area. One of the most important of the Federal initiatives was the recent OPM release of the Parenthetical Classification Titles and Competency-Based Job Profile (Qualification Standard) for the Computer Specialist Series

GS-0334 and the Telecommunications Series GS-0391. These new standards will dramatically improve the ability to manage the civilian IA workforce.

All CINCs, Services and Agencies (C/S/A) have realized the importance of properly trained personnel in the IA area and have committed significant resources to improving the overall status of education, training and awareness of Departmental and contract personnel performing key IA functions.

Specifics regarding each C/S/A's activities in this area are reported in their respective sections of this report. Those activities which were DoD-wide during FY2000 are discussed in the paragraphs below.

DoD took major strides towards the accomplishment of the initial set of IA training and certification requirements with an expected completion (for reporting purposes of this requirement) in the second quarter FY2001. These requirements were established by the June 1998 Memo signed by the Deputy Secretary of Defense (DEPSECDEF), Dr. Hamre. Not only did all of the DoD activities make significant progress in establishing these minimum requirements, they also institutionalized them within their normal training cycles to account for regular turnover of military personnel and civilian personnel changes.

The Information Assurance (IA) and Information Technology (IT) Human Resources Integrated Process Team (IA/IT HRM IPT) finished their analysis and report on IT/IA HR practices in August 1999. In their report, they recommended 19 actions, which when implemented, will significantly improve the training, certification and personnel management of the Department's IT/IA workforce. The recommendations include the following actions:

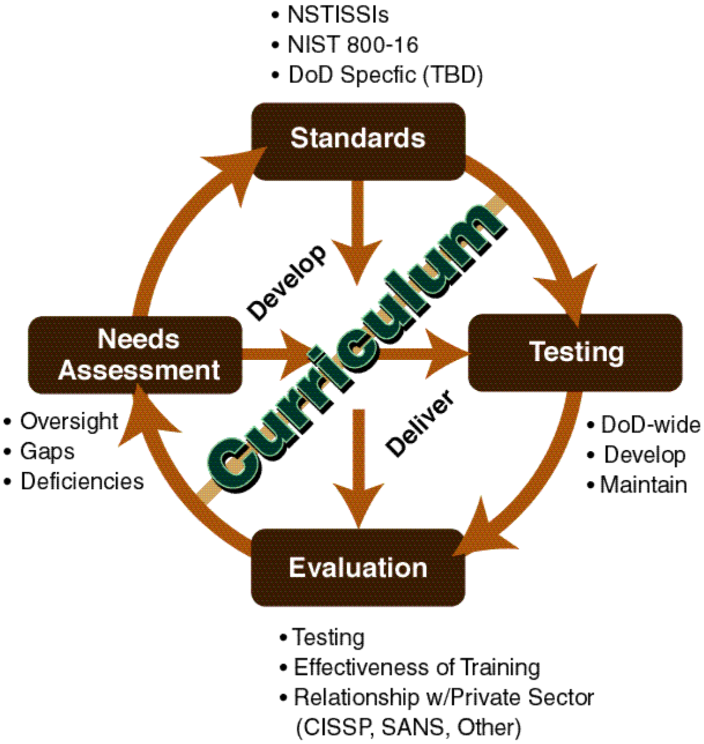


Figure 3

- Changing the manpower and personnel databases to track personnel with IT/IA expertise performing IT/IA functions
- Determine and implement recruiting and retention incentives for military and civilian personnel in IT/IA specialties
- Establish minimum mandatory education and training requirements for personnel in IA functions

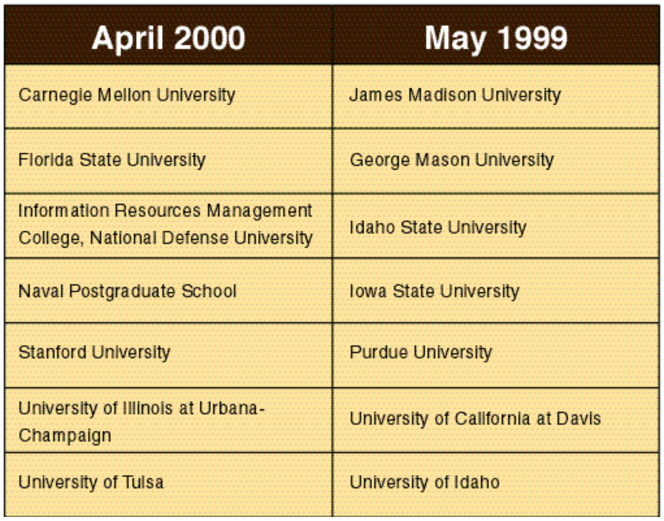
- Standardize criteria for certification of personnel performing IA functions
- Include contractor personnel in tracking, training and certification requirements

These recommendations were approved in a 14 June 2000 Memorandum signed by the DEPSECDEF, Mr. de Leon. The follow-on actions to this Memorandum will be the development of implementation plans for each of the recommendations by the offices of primary responsibility (OPR) on the staff of the Office of the Secretary of Defense. These actions are ongoing as the period of this report closes.

To establish a continuum of education, training and professionalization for the IA workforce, a strawman model process is being developed which accounts for all 11 of the IA functions identified in the 1999 IT/IA IPT. Those functions for which certification criteria have already been developed (Systems Administrator, CERT team members and Red Teams) will be used as the model for developing the remaining IA functions. The process model is at Figure 3.

To assist in the training and awareness initiatives, the DISA Information Assurance Program Office (IAPMO) produced a number of IA computer-based training CDs and video-tapes, available to all Federal activities. These CBTs provide the baseline training for the majority of the Department, making best use of technology to reach personnel throughout the world. More details are provided in the DISA section of the report.

NSA initiated the Centers of Academic Excellence in IA Education in 1999 in an effort to promote higher education in IA and provide the foundation for training security professionals that will supplement the needs of both government and industry. The program was expanded in 2000 to include 14 universities. These universities were selected based on the depth and maturity of their security programs in accordance with the standards developed by the National Security Telecommunications and Information Systems Security Committee (NSTISSC). The Centers of Excellence are listed in the following table:



April 2000	May 1999
Carnegie Mellon University	James Madison University
Florida State University	George Mason University
Information Resources Management College, National Defense University	Idaho State University
Naval Postgraduate School	Iowa State University
Stanford University	Purdue University
University of Illinois at Urbana-Champaign	University of California at Davis
University of Tulsa	University of Idaho

Figure 4. Centers of Academic Excellence

SECURITY MAN AGEMENT INFRASTRUCTURE

Security Management Infrastructure (SMI) provides the framework and services that provide for the overall security of an information infrastructure. SMI includes the Key Management Infrastructure (KMI) plus additional services associated with security applications, the common operating environment (e.g., operating system security), software downloading, auditing, intrusion detection, and password management.

KMI provides the framework and services that provide for the secure creation, distribution, and management of public key products, traditional symmetric keys, and manual cryptographic systems. While KMI includes the Public Key Infrastructure (PKI), KMI supplies a broader range of cryptographic material and supporting services. Intense planning was initiated in FY2000 for KMI to be implemented in an evolutionary manner as a series of "capability increments" (CIs). Each capability increment will build on the capabilities of preceding increments, fielding new or enhanced KMI capabilities to meet the needs of DoD systems in use at the time of that CI.

PKI provides the framework and services that provide for the secure creation, distribution, control, and management of public key products, primarily X.509 certificates. PKI includes the Registration Authority (RA) workstations, the Certificate Authority (CA) workstations, and the archives for key recovery. PKI is an enabling infrastructure and as such supports the operation of PK-enabled software applications, devices, and network directory services.

In September 2000, NSA in conjunction with the DoD CINC's, Services, and Agencies (C/S/A's) was tasked to develop a programmatic COMSEC Cryptographic Modernization Roadmap. A COMSEC Cryptographic Modernization Working Group was assembled from each of the C/S/A's to collaborate on this effort. Modernization drivers include updating aging cryptography and cryptographic products, increased interoperability requirements with allied/coalition, government and industr y, and "new" and emerging network-centric communications architectures requiring advanced cryptographic techniques.

Most of this past year's SMI activity centered on PKI. In accordance with the DoD's IA initiatives, policy regarding the enabling of applications and systems for use on the DoD PKI was drafted in November 1999 and finalized in October 2000. This policy was formulated to address the various milestones and timelines set forth in the PKI Roadmap.

An initial effort was made to calculate the costs of enabling application for the DoD PKI, and a model was constructed for a standardized method for identifying and calculating the cost of public key enabling of applications.

Estimates represented a one-time enabling of each specific application. Life-cycle training and other associated costs, assumed as part of the normal cost of modifying any IT application, were not included in these estimates. Subsequently, DIAP led a working group that managed the collection and analysis of PKI cost data and, on that basis, prepared in April 2000 a report entitled "Review of DoD Public Key Enabling of Applications for FY 2001–2007."

The working group received 690 applications selected by Components to be PK-enabled. It received cost estimates from three Services, one Unified Command, ten Defense Agencies, and one Principal Staff Assistant (PSA). Defense-wide estimated costs to PK-enable these applications were estimated to be a total cost of $175 million (M) ($61M in FY 2001, $43M in FY 2002, and $71M during FY 2003 through 2007.)

Of the several major findings, one concluded that there is a general lack of understanding of PKE at the working level and not enough applications submitted by CINCs, Services, and Agencies. Additional input was provided in June 2000, increasing the estimated FY 2001–2007 total to $191M. A revised draft PKE policy will be out for coordination in early FY 2001. These requirements will continue to be refined through the normal budgeting process.

In November 1999, the Deputy Secretary of Defense also released a policy memorandum entitled "Smart Card Adoption and Implementation." This policy mandated that the common access card (CAC) would serve as DoD’s primary platform for the authentication token to be used for certificates and private keys for digital signature and access control.

An FY 2000 PKI Front-End Assessment (FEA) was chaired on behalf of PA&E and ASD(C3I) from February through May 2000. Participants included NSA, DISA, Services, NIMA, DLA, DIAP, BMDO, DoD Health Affairs, PKI PMO, Smart Card PMO, DMS PMO, DTS, DeCA, and DFAS. The FEA was convened to identify opportunities for consolidating requirements for tokens/CACs, Registration Authority workstations, directories and databases, certification authorities operating personnel in order to achieve the most efficient economies of scale and to consider programmatic alternatives for most efficiently meeting current policies.

Based upon current and anticipated Program Objective Memorandum (POM) data and the findings of the 1999 PKI FEA, participants established a baseline of currently programmed resources for the PKI, Smart Card, Defense Messaging Service, Defense Travel Service, and Electronic Business-Electronic Commerce programs. Participants also identified numerous technical issues that could impact the current PKI/smart card schedule, product availability, or interchangeability. After considering and evaluating several enterprise-wide alternatives, the group recommended an initial postponement of 14 months in the full deployment of the infrastructure, a 12-month postponement in the issuance of Class 3 certificates, and a 9-month postponement in the issuance of Class 4 certificates. The transition to Class 4 for mission-critical systems was postponed by 12 months, and the continued issuance of Class 3 certificates was extended for 3 years, concurrent with the Class 4 deployment. The panel also agreed to recommend that in the near term, Class 3 certificates would continue to be issued on both software and hardware tokens to ease subsequent transition to the use of smart cards as the primary token.

Through weekly discussions, the group worked to identify and achieve the desired capabilities and to take advantage of consolidation opportunities. They considered alternatives that met the current policy, as well as alternatives that would require modifications to the current schedule and/or reductions in the level of mandated assurance. The group considered these alternatives in the context of the overall direct cost impact, the per FY cost impact, the indirect (qualitative, personnel, logistics) cost impact, the initial and long-term scheduling impact, the technical risks, the commercial off-the-shelf supportability, the effect on security posture, and the reusability of existing components. After evaluating all factors and alternatives, the group reached consensus to deploy the Class 3 PKI with a non-Class 4-compliant CAC, with migration to Class 4 PKI using a Class 4-compliant CAC. This choice would create a default assurance level for Class 3 based on the lower level of security provided by a software token, rather than on the higher level of security provided by the hardware token.

The ASD(C3I) embodied the recommendations of the FEA group in its 12 August 2000 PKI Memorandum.

READINESS

DIAP's Readiness assessment team has made great strides during FY 2000. Early in its existence, the Readiness assessment team identified the overarching objective of developing and implementing a methodology and a capability for assessing the DoD's IA Readiness status. Concurrently, the team began identifying challenges to meet and obstacles to overcome in order to put into place that methodology and capability.

IA GOALS

The first step in IA Readiness assessment methodology and capability is to develop a DoD-wide process and associated metrics by which the Secretary of Defense (SECDEF) and the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [ASD(C3I)] can objectively measure and articulate the Department's IA Readiness status. The second step is to include functionality in the process so that it will provide useful information that will help identify and support IA resource requirements.

Many challenges and obstacles must be overcome before a DoD-wide IA Readiness assessment methodology can be completed successfully. The first of two primary goals therefore is to develop this capability through a structured methodology that will provide relevant, adequate data usable by all DoD Components. IA effectiveness measurement will serve as a basis for analysis to support planning IA capabilities, strategies, and procedures and to ensure protection of the information segment of our warfighting resources.

Member of the 442nd Fighter Wing straps and buckles up for flight.

The second primary goal will be to increase IA visibility within the IA Readiness assessment process. Currently, IA has limited visibility within the Planning Programming, and Budgeting System (PPBS) process. The IA Readiness assessment methodology must be structured to provide relevant, adequate data to enable DIAP to make an effective business case for IA and to make IA investments fiscally defensible.

Readiness Assessment Concepts

Immediately following its inception, DIAP's Readiness team began developing a strawman IA Readiness assessment concept framework. Early in calendar year 2000, it began coordinating the framework with DoD Component IA representatives. The coordination effort had a dual purpose: to disseminate framework details for feedback and to recruit participation in a workshop held during summer 2000.As part of the conceptual framework, the Readiness team developed the following proposed definition of IA readiness: "the measured ability of DoD information technology systems, embedded information technologies, and their related infrastructures to withstand incidents and attacks and to provide effective support to execution of the Department's combat and noncombat missions." That definition was subsequently proposed to workshop participants as a starting point for adopting a formal definition of IA Readiness.

The methodology used in structuring metrics for the IA Readiness assessment concept framework was built upon three main tenets: organization, aggregation, and scoring. Organization is how operational commanders organize and prioritize their assets for conducting their warfighting mission. Aggregation, which comprises three distinct assessment levels, addresses the utility of generating and managing IA concepts within long (executive), medium (management), and short (operational) time frames. The scoring structure emulates the Status of Operational Readiness and Training System (SORTS) structure, with ratings ranging from C1 (excellent) to C4 (unacceptable). DIAP's Readiness team conducted (12–14 July 2000) a workshop entitled "IA Readiness Assessment Metrics," with substantial Component representation and support. Using the strawman Readiness assessment framework as a starting point, the 21 participants produced a draft IA Readiness assessment framework during the three-day period (the draft remains under development). At the request of Component representatives participating in the workshop, DIAP formed, with Information Assurance Panel approval, an IA Readiness Metrics Working Group to formalize and provide continuity for the activities and products of the Readiness workshop.

One of the products of the workshop was a draft working definition of IA Readiness as "the measured ability of DoD's information capabilities within its mission-critical, mission-support, and administrative systems, and their associated infrastructures, including people, processes, policy, equipment, and technology, to assure operational effectiveness in executing combat and noncombat missions. This includes robust operations under attack, failure, and operational errors, as well as endurance and an ability to reconstitute under all conditions."

Workshop participants also developed a formal goal statement for the framework that supports the Joint Staff's Joint Vision 2020: "DoD's Information Assurance ensures sufficiently resilient and operationally effective information capabilities to support information superiority and mission operations across the full spectrum of combat."

Critical Success Indicators

Workshop participants also developed critical success indicators (CSIs) that correlate to the highest level of IA Readiness metrics and that are indicators used to determine the measure of success for each of the highest-level metrics. The draft CSIs are organized as categories of metrics relating to the manner in which operational commanders organize their assets for prioritization and management: People, Operations, Training, Equipment and Infrastructure, and Processes.As a result of input from workshop participants, the IA Readiness Metrics Working Group was established in September 2000 to serve as the DoD's lead organization to research, develop, identify, validate, test, and recommend metrics applicable to the IA Readiness assessment process.

The working group has taken on many different projects associated with the development of IA Readiness efforts. It is identifying and reviewing feasible and relevant metrics for use in assessing the DoD's IA Readiness status and then prioritizing them as candidate metrics. Based upon this prioritization, it will recommend to DIAP the most appropriate metrics. It is also reviewing existing IA metrics for continued use, modification, or discontinuation. All metrics-related work is completed through Component staff coordination.

Working in Rapid Reaction Corps HQ, Bosnia.

Further development and implementation of the DoD-wide IA Readiness assessment process will be an effort over several years. It will require additional DIAP resources and close coordination throughout the DoD. To organize and facilitate its efforts, the Readiness team has identified the following interrelated functions and activities to be performed in a coordinated manner for the successful development of an IA Readiness assessment capability: Framework Development Coordination and Management; Metrics Development and Testing; Process Review, Modification, and Development; and Policy Review, Modification, and Development.

The successful implementation of an effective IA Readiness assessment process is expected to provide the following benefits: an objective picture of the DoD's IA Readiness status; identification and validation of IA resource requirements; identification of substantive input to DoD policy formulation; and constructive feedback to managers and the IT community.

ARCHITECTURE

Many efforts, both near- and far-term, are ongoing in developing information system architectures and their related IA architectures. This section addresses the more significant of those IA architecture efforts being performed by CINCs/Services/Agencies. Among these are the Global Information Grid (GIG) Information Assurance Architecture Working Group (IAAWG) under the aegis of ASD(C3I), the IA Technical Framework (IATF) being developed under the sponsorship of NSA, the nearer-term DISN IA architecture being developed by DISA, the NetOps Pilot activities at USPACOM, and nearer-term IA architectural improvements being developed by the Services.

Information Assurance Architecture Working Group

The efforts of the GIG IAAWG began in late FY 1999. The IAAWG membership comprises participants from DoD, Federally Funded Research and Development Centers (FFRDCs), and DoD contractors.

The initial set of IAAWG products, provided at the end of March 2000, comprised prototype overlays to USPACOM, current and future operational-architecture views; a required update to incorporate IA properties into the DoD C4ISR Architecture Framework Document; and a compilation of lessons learned from this initial prototyping effort.

Most significant within this effort was the incorporation of the concept of NetOps into the future prototype overlay. "NetOps" is defined as the closer coupling or tighter integration of the functions of information assurance, telecommunications network management, and information dissemination management. Operationally, NetOps captures in one overall concept, the Commander’s need to visualize and control all information flows over warfighting, warfighting support, and/or business networks within an Area of Responsibility (AOR) (e.g., the Pacific AOR). This set of information allows the GIG architects, working in concert with the C/S/As, to develop and evaluate various process alternatives to support NetOps functions. In the next phase of architectural development, designed to assess NetOps Management Center (NMC) feasibility, efficiency, and effectiveness, IAAWG will examine the concept of operationally tiered, "virtually structured," collaborative NMCs capable of providing more focused theater and regional support.

A critical tie between architectures and operations is the use of architectural data in support of operations which will create a responsive, decisive, and survivable warfighting capability. Attaining the capabilities envisioned in the NetOps concept will enable rapid decisive operations (RDO) in which various elements of a joint force can be quickly assembled and interconnected to plan and execute warfighting operations or mission operations other than warfare. Enabling RDO is a major potential benefit of the use of architectures within DoD.

The IAAWG believes that the NetOps overlay components can largely be reused to support other operational architecture views. To demonstrate this potential component reusability, the IAAWG is analyzing the Defense Finance and Accounting System (DFAS) operations to determine the degree of reusable NetOps components.. This examination covers both the DFAS organizational operations and the DISA Defense Enterprise Computing Centers supporting those operations. It is anticipated that this examination will be completed early in 2001 and that the results will demonstrate general extensibility of NetOps overlays to the operational views of DoD electronic commerce/electronic business architectures.

IA Technical Framework

A key vehicle both for promoting awareness of, and for providing guidance on IA is the National Security Agency's (NSA's) Information Assurance Technical Framework (IATF) document. This unclassified compendium of IA concerns, approaches, and general guidance has evolved in harmony with the work of the Chief Information Officer (CIO), including the IAAWG. Its target audiences range from system security engineers (SSEs) to IT managers and from Federal to industry executives.

During 2000, NSA significantly updated the IATF document with the development of Release 3.0. This release, dated September 2000, is fully aligned with the DoD's Defense in Depth Strategy for implementation of IA. It contains new material, including uses and implementation of KMI and PKI information protection mechanisms. The IATF document addresses numerous IA topics, including the four technology-area facets of the Defense in Depth Strategy The document provides a foundation of "how to" information for individuals implementing the operational IA architecture developed by the GIG IAAWG.

The IATF document also has some preliminary material on the integrated approach to NetOps within the DoD. During the next year—as the GIG IAAWG furthers the architectural definition of NetOps for DoD—the NSA plans to add material on security management to the IATF document.

The IATF document can be obtained at www.iatf.net, a website accessible to members of the IATF Forum, an NSA outreach activity with other U.S. Government organizations and U.S. industry. The document has also been extensively distributed on CD-ROM.

OPERATIONS

The DIAP Operational Environment (DIAP-OE) oversees the daily management and the operational capabilities that establish and maintain DoD's Information Assurance (IA) posture. In FY 2000, particular attention was paid to IA monitoring and network management IA tools because these are the sources of information for day-to-day operational management actions. Operational management and determination of future capabilities depend on the quality and the wide-scale deployment of IA monitoring and network management and their configurations.

FY 2000 saw numerous activities related to the immediate, mid-, and long-term needs of IA operations, producing results through several approaches. One was to address immediate problems or specific issues through the Information Assurance Panel (IAP) of the Military Communications and Electronics Board (MCEB). A second approach was to improve management capabilities in order to understand the vulnerabilities of our systems and operations and to provide mitigation solutions. A third was to initiate activities to improve future operational capabilities critical to survivable and sustainable operations. These activities included the following:

- IAP Operational Tasking
  - Ports and Protocols Registry
  - Mobile Code
  - IA Tools Inventory
- Vulnerability Management and Mitigation
  - DIO-CND Study
  - IAVA
  - Current Mitigation Efforts
- Future Operational Capabilities
  - Attack Sensing and Warning (AS&W)
  - Enterprise Sensor Grid (ESG)
  - Joint Experimentation and Exercises

IAP Operational Tasking

As all communities, the Operational Community must respond in the near term to actual and perceived problems while constrained by available resources. The DIAP-OE generally responds to such issues through the IAP. The IAP of the Military Communications - Electronics Board (MCEB) allows the DIAP-OE to examine near-term situations and to address specific and immediate problems that the operational communities cannot resolve alone. Furthermore, for solutions to be both affordable and effective enterprisewide, they usually require shared implementation, and they benefit from shared experience and knowledge to improve the DoD IA posture. A number of successful results were obtained this year:

- **Ports and Protocols Registry**
  In the course of the year, numerous operational problems occurred that could be traced to the unmanaged use of unassigned

ports and protocols. The Defense Travel System (DTS) Program Manager first noted the need to discipline the use of ports in order for the DTS to properly operate. The value of the DTS was strongly tied to achieving enterprisewide interoperation among various networks and systems. Further examination also indicated that leaving the resolution of this issue to individuals not only caused program operational problems but would also subject DoD to major vulnerabilities. Consequently, the IAP decided to develop a definition, policy recommendations, and operational procedures. These would ensure that programs and systems throughout DoD could offer needed capabilities while, at the same time, mitigating the enterprisewide risks of undisciplined use of computing and of the network ports and protocols that provide the fundamental interfaces among domains. Further advances in this management capability are expected next year.

- **Mobile Code**
  Mobile Code is software obtained from remote systems outside the enclave boundary, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by a recipient. This past year, numerous incidents exploited mobile code vulnerabilities. The agencies most affected have been those whose operations are strongly dependent on the features that mobile code enables, but that also open vulnerabilities to exploitation. Examples of these are distance learning, e-commerce, and logistics. A common operational characteristic of these operations is their need to interact outside DoD. Various solutions are under investigation for diminishing the potential for mobile code while continuing to benefit from the technology. As part of the IAP Defense in Depth efforts, the IAP developed a policy for operations throughout the enterprise. This effort will continue as experience is gained in regard to policy compliance and as technologies evolve toward higher levels of assurance and security.

- **IA Tools Inventory**
  Operational community collaboration began with tasking the IAP with surveying the IA tools in use by the CINCs, Services, and Agencies (C/S/As). Sharing experience and information on the state and condition of DoD’s IA posture must begin by establishing a database of capabilities for comparative ability purposes. Once established, this database also provides a basis for better understanding the operational deficiencies indicated by the deployed equipment and tools and serves to inform other DIAP areas of needed R&D, acquisition or policy, and procedural changes. This effort began late in FY 2000 and will continue in FY 2001.

In this initial effort toward standardization of IA tool sets, many of the C/S/As have established IA configuration baselines. The DoD is presently reviewing common and best practices for IA, with the goal of establishing guidelines and oversight management instructions and directives. During FY 2000, considerable progress has been made in the areas of policy and instruction. Rapidly emerging technology will continue to create a need for improvements in IA and will remain a major evolving challenge for the foreseeable future.

Vulnerability Management and Mitigation

Overall, vulnerability management in FY 2000 gave the DoD an operational visibility that established the pervasive nature of assuring information throughout the enterprise. Activities improved the provision of facts and evidence for the actual or potential consequences of failure. This information helps to establish sound requirements and to exploit emerging opportunities in technologies, techniques, and procedures.

Sensing capabilities are critical to ensuring that networks and systems are protected and that responsive actions are taken when attacks occur, but many attacks succeed or are enabled when known vulnerabilities remain unattended. The IAP has undertaken to examine whether DoD manages known vulnerabilities adequately and addresses them throughout the Department in a timely and affordable manner. This effort entailed examining the existing processes that provide information to systems administrators, operators, and users of operational systems such as the IAVA process, INFOCON alerts, and Certification and Accreditation (C&A) of operations discussed below.

In general, significant progress was made and continues to be made. Such visibility makes evident to all DoD personnel that operational vulnerabilities anywhere in DoD can, if exploited, result in significant problems. This is particularly the case when they propagate well beyond the boundaries of systems and networks too often viewed by individual users and operators as isolated failures. In FY 2000, progress in this area has generally resulted in the following:

- Increased compliance with IAVA alerts
- Increased awareness of the need to actively monitor compliance, supported by automation
- Increased awareness of the need to comply with, and act upon, DITSCAP versus issuance of waivers
- Growing sensitivity to the issues of configuration management as a critical factor in operations management of networks and the information-based systems that depend on them

In FY 2000, the DIO-CND study established a broad foundation for Computer Network Defense (CND) and the policy needs to support clear separation of CND and Computer Network

Attack (CNA) information operations. This foundation also provides a basis for developing future resource justifications and to programmatically assess the mitigation of operational vulnerabilities and the development of future operational capabilities.

Two management processes were addressed in FY 2000, with improving results: the Information Assurance Vulnerability Alert (IAVA) process and the INFOCON process. As the year has progressed, the IAVA process has seen improved reporting and acknowledgement of vulnerabilities by system administrators. The IAP is expected to continue to develop improved methods and means to ensure timely management response to vulnerability discoveries and notifications to mitigate them. Enterprisewide, the INFOCON process provides a means to communicate to users that operations are vulnerable or under duress. The process still has shortfalls that will be addressed in FY 2001.

DIO-CND Study

The ASD(C3I) completed a comprehensive study of Defensive Information Operations – Computer Network Defense (DIO-CND) and moved to the final phase of its efforts to identify core CND functions, recommend integrated policy and responsibilities, and develop a programmatic structure for POMs. As a direct result of this effort, a draft DoD Instruction and Directive were written and are undergoing formal review. This, added to a CND study to evaluate the overall state of the DoD, enabled the Department to gain a better picture and understanding of the health of the many and varied elements that constitute the CND, its network, and its systems.

Information Assurance Vulnerability Alert

ASD(C3I) signed and released a memorandum in May 2000 with the intent of providing coordination and distribution of the many Information Assurance Vulnerability Alert (IAVA) products that the DoD receives on a routine basis. The objectives set forth in the memorandum are being incorporated as part of the DIO-CND instruction. An IAVA distribution system was created for the release of alert and warning notices in response to recently discovered vulnerabilities. The intent is that system and network administrators receive these products in the shortest time possible and acknowledge receipt. Actual corrective measures may take longer to incorporate, based upon system and configuration standardization requirements. The effort is considered a major success when the impact of the vulnerability described in the alert is minimized.

The creation of the IAVA process has seen a degree of success and demonstrated that had vulnerabilities identified in the alerts and warning notices been corrected, a large number of intrusions would never have taken place. U.S. Space Command, which has the responsibility of managing the CND and CNA efforts, has conducted recent conferences to create a more effective IAVA process. The goal is not only receipt notification but also actual problem resolution in a matter of hours.

Current Mitigation Efforts

While the protection of individual military systems is important, emphasis is shifting from the protection of these systems to a more dynamic management of all IA resources. The protection philosophy for the interconnecting networks follows this same approach. The majority of information systems used within the DoD consist of mostly commercial off-the-shelf (COTS) products; configuration of these products in a secure manner is of prime importance. ASD/OSD are providing the overall management documents to support the many programs and projects within the DoD.

The Department realizes that protecting networks offers a greater degree of protection than simply protecting individual systems. In other words, networks establish families of systems that result in exploitation opportunities that otherwise may be more difficult to realize or not possible. Managers throughout DoD understand that for this revised protection philosophy to succeed, protection schemes must be adjustable and must have the ability to be totally reallocated or retargeted in relatively short time frames. Attacks and probes into the DoD systems and networks come with no advance notice and usually last a very short time. These conditions dictate a dynamic management philosophy.

Recent efforts to improve the overall protection of the networks and systems have resulted in many Services and Agencies deploying intrusion detection systems (IDSs) and firewalls for the first time. Others have gone further, increasing the complexity and depth of coverage. The present philosophy is to use IDSs and firewalls in conjunction to provide an improved safety net between the Internet and DoD networks; however, these systems are only as good as the management procedures and processes used to support them. To complement them, the DoD is also increasing the number of Computer Emergency/Incident Response Teams (CERTs/CIRTs), Regional Computer Emergency Response Teams (RCERTs), Network Operations and Security Centers (NOSCs), and Network Operations Centers (NOCs).

These centers are the hub of the detection and analysis framework for the DoD. This is where data from the IDSs and firewalls are analyzed. This analysis provides the basis for the study of trends, as well as for the detection of intrusion attempts and actual intrusions. Data from these systems are seen both in real time and near real time and in daily core dumps. The role of the CERTs, RCERTs, NOSCs, and NOCs is to provide the depth of expert talent and automation needed to analyze and correlate the data, with a resulting increase in the number of centers and personnel to support them.

Future Operational Capabilities

The corporate use of IDSs and firewalls has brought to light the present situation in which DoD now finds itself with an extensive Enterprise Sensor Grid (ESG). Service elements and Agencies that in the past could simply keep everything in-house now find that risk is mutual and shared. This situation dictates that information from the IDSs and firewalls also be shared and indicates that DoD can now corporately distribute assets more efficiently and more economically. These efforts have set the stage for the DoD to create a joint database that defines the elements of the ESG and the data it contains:

- **Attack Sensing and Warning (AS&W)**
  One of the more difficult tasks of the operator is to determine that computer networks and systems are under cyberattack. Attack implies the ability to attribute the actions to a motivated adversary versus the inability to target the source. The difficulty of attribution notwithstanding, progress was made toward adequately characterizing the data requirements and tasks necessary to give to the leadership enough sensing capabilities and warning of a potential attack. Details are largely classified.

  Many areas such as Attack Sensing and Warning and the realization of the new CND/CNA roles and responsibilities are just now beginning to be defined. CND is the most defined of the group, with USSPACECOM taking the lead. CNA and AS&W are just now beginning to be defined; it is too early in the process to address these.

- **Enterprise Sensor Grid (ESG)**
  During the 4th Annual IA Workshop, Defensive Information Operations (DIO) track, a number of issues were developed. Included in this effort was Issue 11: Enterprise Sensor Grid Management. The action item was to sponsor a DoD-wide technical workshop/conference to determine a DoD signature detection baseline, to create a protected distribution method, and to develop a global view of network coverage. The objective of this effort is to

  - Share the current IDS capabilities and strategies across the Services and Agencies with operational IDS programs,
  - Gain industry perspectives about their visions of future IDS technology, and
  - Gather requirements to support an IDS enterprise software initiative.

The IDS Workshop outcomes were the following:

- Validate ID operational requirements through a 32-features survey given to vendors and attendees

- Identify gaps in DII-wide sensor grid coverage that would inform the development of a strategy to archive and share signature files among Services and Agencies
- Document security profile requirements for IDSs
- Build consensus for IDS enterprise licenses(s)

The survey was completed in August 2000 and given to the NIAP and the Protection Profile activity of the Common Criteria activity. The sensor coverage action has defined a prototype based on the Lawrence Livermore process of signature dissemination and is currently developing it. The strategy is to adapt this method to DoD and explore its applicability. Implementation is expected in the first quarter of FY 2001. A parallel effort has generated data from the Services and Agencies, characterizing the information that they are able to share and associated restrictions. This provides the basis for an eventual expansion to the full network of the sensor grid, through a gap analysis. This critical operational capability to sense the state of DoD’s networks and respond appropriately will be further examined at the 5th Annual IA Workshop in February 2001.

Coincident with this effort, the Information Assurance Panel (IAP) of the MCEB initiated a tools survey of its membership. This information will also be used to inform the ESG efforts.

- **Joint Experimentation and Exercises** Operational value is under constant scrutiny through joint experimentation involving users, operators, and developers. In FY 2000, IA began to be addressed through this traditional mechanism for connecting requirements with developments in deployed environments. By and large, these exercises and experiments demonstrated the value of capabilities toward achieving information superiority (IS). However, better means will be required in the future to deal with rapid technology expiration rates, both in information technologies (ITs) that drive IA, as well as IA tactics, techniques, and procedures or technologies. This may require developing new methods that support opportunistic approaches to making operational advancements, rather than relying exclusively on the traditional requirements generation, acquisition development, and deployment processes of the Department. Formal processes can only meet slow technology evolution and well-characterized threats.

Information Assurance is achieved in an environment where potential threats and vulnerabilities from technologies are constantly changing. Experimentation and exercises offer the advantage of quickly gaining experience in an environment as realistic as possible and of improving judgment of when, where, and how much DoD must deploy new IA capabilities to achieve information superiority.

RESEARCH AND DEVELOPMENT

Technology plays a crucial role within the Department of Defense. In order to achieve Full Spectrum Dominance, as outlined in Joint Vision 2020, the U.S. military needs not only capable personnel and sound tactics but also the best tools available to perform its mission. In order to develop the best technologies for the best value, DoD has partnered with many technology companies. However, it also seeks to develop many technologies of its own.

FY 2000 brought forth a myriad of IA and Critical Infrastructure Protection (CIP) research and development (R&D) activities throughout the Department. These ranged from improved cross-organizational coordination activities to the revamping of individual agency R&D programs. The activities comprise numerous workshops, efforts to effect technology transition, cofunding of research projects, and initiation of a broad set of IA research projects.

Defense Science and Technology

Information Assurance Science and Technology (S&T) for the Services and Defense Agencies is coordinated through the Defense S&T Reliance planning process. Reliance is under the strategic oversight of the Office of the Deputy Under Secretary of Defense for Science and Technology. The Information Assurance Subarea of the Information Systems Technology Area is developing the technologies and architectures needed to provide warfighters with a secure and survivable C4I information infrastructure. The infrastructure must be highly automated, adaptive, resource managed, and resilient to attacks of all types.

Major S&T challenges, which are currently being addressed, include:

Assurance Methodologies:

(1) Detecting subtle information integrity attacks, developing algorithms for self-repair, and creating techniques to map mission-critical services to remaining trustworthy resources;

(2) quantifying and analyzing security and survivability requirements and assessing the degree of compliance and assurance achieved.

Cyber Panel:

(1) Designing attack detection sensors and sensor placement and developing the correlation algorithms to detect highly sophisticated stealthy distributed attacks spread out over time and space;

(2) allowing operators to monitor the operation and attack state of information systems and networks on which they depend, at theater scales and in operationally relevant terms, and to observe and manipulate the operation of security and survivability features;

(3) modeling of system and application configuration and resource requirements while accounting for dynamic characteristics such as migration of mobile

processing or operation of automatic load-balancing or failover features;

(4) the creation of rich and general models of coordinated and large-scale attacks, rather than the low level and anecdotal representations that now exist;

(5) validation of network monitoring and response research efforts.

Organicall y Assured and Survivia ble Information Systems:

(1) Ensuring the continued availability and graceful degradation of the system under partially successful attacks, minimizing resources available to attackers while maximizing the residual capacity available to legitimate users;

(2) determining the difference between malicious and accidental faults;

(3) effectively integrating the resulting wide variety of intrusion detection, correlation, intrusion tolerance, and response technologies to provide the maximum possible protection while simultaneously minimizing the performance degradation and additional cost incurred by these mechanisms.

Survivable Wired and Wireless Infrastructure for Military Operation: Creating a trustworthy infrastructure that will support Netcentric operations and is capable of operating through sustained computer network attack.

Fault Tolerant Networks:

(1) Eliminating network services single points of failure;

(2) fortifying network elements to defeat or resist denial of service attacks;

(3) developing tools and techniques to restore degraded networks to an acceptable operating level.

Dynamic Management/Joint Coalition:

(1) Enabling secure collaboration within dynamically established mission-specific coalitions while minimizing potential threats from increased exposure or compromised partners;

(2) developing secure group management protocols.

Basic research is being directed at the fundamental science problems of this subarea in numerous areas: streaming media protection techniques, steganographic detection algorithms (methods of hiding the existence of a message or other data), watermarking methods for tamper resistance, mobile code protection and authentication methods.

INFOSEC Research Council

Several of these coordination activities revolved around the INFOSEC Research Council (IRC). A self-chartered coordination body of U.S. Government sponsors of information security research, the IRC has evolved from being solely DoD to a group that now spans a greater portion of the Federal Government. Today the

IRC coordinates, collaborates, and influences IA research within and among the DoD (Defense Advanced Research Projects Agency, National Security Agency, Army, Navy, and Air Force), the intelligence community, and Federal civil agencies [Department of Energy (DoE), Department of Commerce (DoC), and others]. In the past year, it has attracted participation from the National Science Foundation, Office of Science and Technology Policy, Chief Information Assurance Officer, Director, Defense Research and Engineering, Advanced Research and Development Activity (ARDA), and the Justice Department.

The IRC provides its members with a community-wide forum to discuss critical information security issues, convey the research needs of their respective communities, and describe current research initiatives and proposed courses of action for future research investments. It also serves as a means to advocate future IA R&D. The IRC sets the example for meeting cross-organizational and cooperative and collaborative demands within a DIAP functional area (IA R&D). This is the first organization of its type in support of IA, but one of several similar functional-area organizations needed to properly implement and institutionalize the Defense-wide IA Program.

In FY 2000, the IRC has, through its Information Security Technology Study Groups, completed a study on an IA Technology Vision, attempting to forecast technology and its effects on IA far into the future (circa 2025). This vision will help in the construction of IA research roadmaps to further assist in IA R&D coordination. One of the IRC's study groups has also conducted a more narrowly targeted study on the problem of malicious code and technologies that may mitigate this problem. A version of this malicious code study was published in IEEE Software in September 2000.

In addition, the IRC has automated its database of member project reports, with the goal of providing information to its members in a more timely and usable form. The INFOSEC Hard Problems List, completed at the end of FY 1999, was briefed to several groups and has stimulated both favorable comment and new research. The IRC has instituted a procedure to keep the INFOSEC Hard Problems List up to date.

Department of Energy

In addition to directly funded R&D from Services or Agencies, the Department of Energy, through its DoE Laboratories, has important INFOSEC collaboration ongoing with the Department of Defense. This collaboration is primarily in the form of cofunding of research in INFOSEC tools and subsequent evaluation and use of those tools throughout both Departments. Among these collaborative efforts are the following:

Automated Patching of Code: This project is focused on achieving greater security of systems by more rapid and thorough correction of fielded software. It also directly addresses the issues of inexperienced or insufficient numbers of system and security administrators.

Network Intrusion Detection (NID) Tool: This project, being conducted by Lawrence-Livermore Laboratory in cooperation with the Army Research Laboratory, focuses on the utility and applicability of the DoE NID tool to Asynchronous Transfer Mode (ATM) and switched networks.

INFOSEC Tool Distribution: This technology transition effort is of continuing benefit to the DoD. DISA has been widely distributing DoE INFOSEC tools such as NID and Security Profile Inspector (SPI) throughout DoD, where they are being used extensively to improve the overall IA posture of the DoD.

Vulnerability Toolkit Components: This effort is coordinated by the interagency Technical Support Working Group (TSWG) sponsored by the DoD's Combating Terrorism Technology Office. Members of this group comprise technology and infrastructure protection experts from DoE, DoD, and the State Department. Among the recently developed technologies that have emerged through this group is the "FLASHROM Vulnerabilities Toolkit," which enables a security administrator to take a snapshot of a FLASHROM and then monitor it over time to detect subversion attempts.

Training Simulators for System and Security Administration (Under Attack): This is another cooperative effort through the TSWG. It addresses the need to provide experience to administrators who know how to administer their systems and networks, but have not had to do so under the pressure of attacks. Two different approaches are being taken: The first builds simulations that can be exercised over an existing UNIX environment, using normal routine administration capabilities and statistically driven simulation scenarios (e.g., simulated phone calls to state that the network is down or that some aspect of the system is not working). The second approach builds a specific networked system that can be used for live attack and defense. It uses commercially available defensive tools and many hacker tools. The training is done in blue (defending) and red (attacking) teams. This is a newly initiated effort for which DoE has a role as task manager.

ACQUISITION

DIAP's Acquisition and Product Support office is responsible for providing continuous improvement to the Department's IA Readiness posture through disciplined, performance-based investments in security-enabled IT acquisitions. These responsibilities begin with the development and implementation of IA-related acquisition guidance, integration of operational requirements documents and mission needs statements, and review of Departmental protection profiles. Other responsibilities include identifying technology, product, and acquisition trends; developing strategies for dealing with the trends; and conducting product evaluation, certification, and integration guidance.

In an effort to expand the influence of the DIAP office on policy formulation, DIAP Acquisition gained admittance to the Defense Acquisition Policy Working Group (DAPWG), the Knowledge Management Working Group (KMWG), and the Information Warfare/Information Security (IW/IS) Council. These groups are major players in the acquisition community and influence acquisition policy development and implementation. DIAP involvement presents a good opportunity to ensure that overall Defensewide IA goals are met.

An IA-specific cost model is currently in development. The cost model will provide a tailored starting point for cost data compilation and will include a breakout of all IA-specific cost and data categories necessary for the development of IA program requirement submissions. The developed model should be completed and testing should start by late spring 2001.

DIAP was selected to present an IA tutorial briefing at the fall 2000 Program Element Officer (PEO)/SYSCOM Conference. The tutorial, titled "Information Assurance: Understanding the Concepts and the Threats," was a joint effort between DIAP and the Defense Threat Reduction Agency (DTRA). It presented two themes: The first centered around the DIAP office providing DoD-wide oversight guidance in IA and actively seeking acquisition community participation in any program-related IA issues. The second regarded DTRA's recent red team/blue team findings that depicted how simple, good intentions on the part of Program Managers can result in sensitive program information falling into the wrong hands and jeopardizing program mission and performance. DIAP's continuing participation in the PEO/SYSCOM Conferences will provide the appropriate forum for acquisition community participation in the understanding of IA and how the IA acquisition functional team can be of assistance.

An initiative currently in development is an IA Tool Set identification and development effort. Under this initiative, the Program Manager (PM), Program Element Officer (PEO), and

Acquisition Executive (AE) communities will be engaged to help identify a complete set of IA tools that can be used in the overall execution of any program. Once this information is gathered, work will begin on a development/procurement effort to create these tools. The IA cost model, already mentioned, is the first step in this process.

DIAP is constantly providing (or seeking to provide) IA subject matter narratives to major DoD acquisition policy modification efforts. This will enable and empower Program Managers to factor in IA requirements and costs much earlier in the acquisition life cycle of their programs. In concert with this effort, they will seek participation with J8/JCS to provide the appropriate forum for the development and refinement of IA doctrine as it applies to acquisition. The Acquisition Group will continually interface with other DIAP functional groups to help promote R&D transition, Architecture transition, Modeling and Simulation development, Test and Evaluation incorporation, Training definition, and Logistics transition.

RESERVE COMPONENT LIAISON

The Reserve Component plays a prominent part in the development and support of the Department of Defense IA posture. Just as Regular forces, Reserves need to maintain secure, real-time communications and share data—both tactical and nontactical—over a secure technical infrastructure. This has been the basic goal of the Reserve IA efforts to date.

The DIAP office is responsible for overseeing the plans, programs, and activities that help to integrate Reserve Components into Defensewide IA operations. The Reserve Component Liaison for IA, a newly created position filled by an Air National Guard officer, has taken active measures to increase IA awareness within the Reserves. The Reserve Component is defined as the Reserve body of each major Service, as well as the Army and Air National Guards. (The Reserve Component's IA activities are detailed below.) Major current initiatives are the Reserve Component Employment Study 2000–2005, the Joint Reserve Component Virtual Information Operations (JRVIO), the integration of DoD IA functions into state Emergency Operations Center (EOC) critical infrastructure protection activities nationally.

United States Army Reserve

The United States Army Reserve (USAR) considers IA a strategic resource to enhance its mission. Over the past year, the Army Reserve Chief Information Office (CIO) has undertaken many initiatives to ensure the USAR's operational success in the twenty-first century. One of the most important has been the development of the Army Reserve Wide Area Enterprise Network (ARNet).

The ARNet has expanded significantly in the past year. It has evolved from a system with only administrative capabilities to one that encompasses mission support functions as well. This mission support includes implementation of systems such as Global Combat Support System - Army (GCSS-A), Defense Integrated Military Human Resource System (DIMHRS), Integrated Total Army Personnel Database (ITAPD), and other e-commerce type systems that will provide the USAR with unprecedented capabilities.

The physical size of the ARNet enterprise network has tripled between 01 October 1998 and 01 October 2000, creating one of the largest wide area network (WAN) implementations in the world. The ARNet comprises more than 1,100 sites within the continental United States and the Caribbean. Its integrated communications capabilities are used by 41,000 Department of the Army (DA), DoD, U.S. Army Forces Command (FORSCOM), National

Guard, and USAR full-time and Reserve personnel. Accounts for 28,500 users are maintained for access to USAR mission-critical and mission-essential systems, as well as the DA Standard Army Management Information System (STAMIS).

From an infrastructure perspective, the ARNet project has completed more than 120 cabling jobs, providing essential infrastructure for network operations. The ARNet enterprise comprises more than 800 routers, 700 PBXs, and 30 ATMs. It has become a key communications medium throughout the Army Reserves, with approximately 5 million e-mail messages passing over the network each week. There are plans to expand and migrate the ARNet to the 7th Army Reserve Command in Germany and the 9th Regional Support Command in Hawaii.

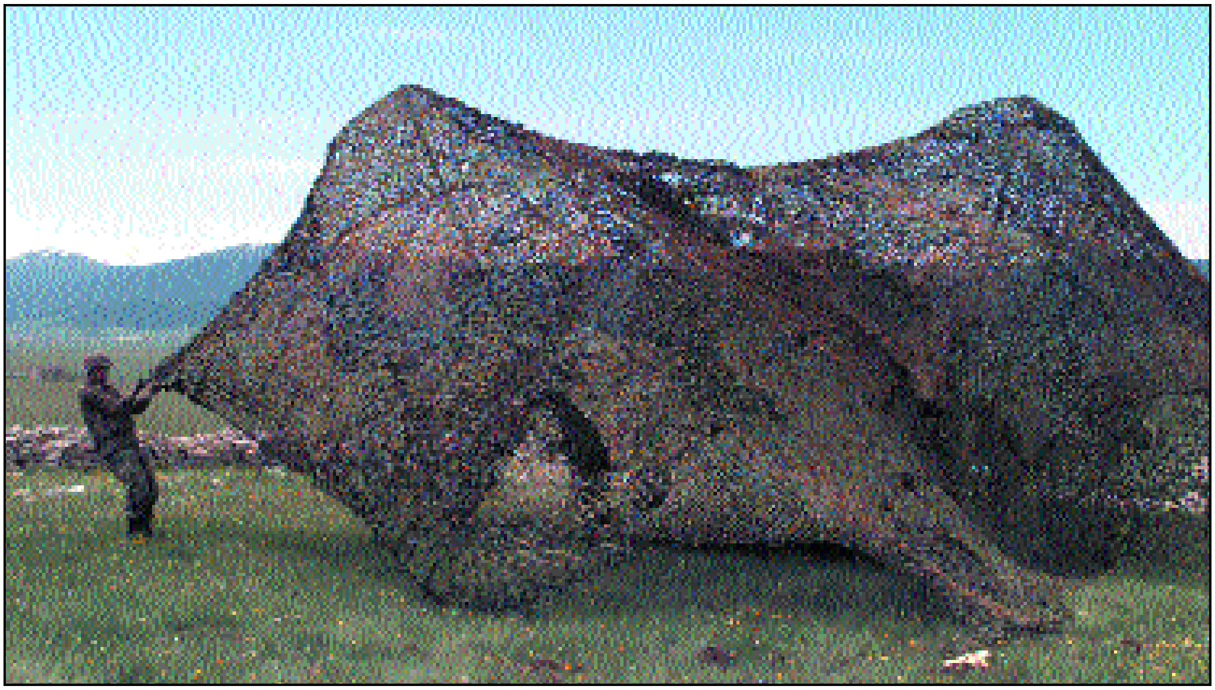
ARNet was fully prepared for the Year 2000 (Y2K) and experienced no problems. Its modification, testing, replacement, and certification of USAR systems was completed well in advance and with no system interruptions or downtime.

The USAR continues to promote IA focus on user training and awareness, ongoing expansion of current security applications and technologies, and implementation of policies and procedures in accordance with DoD requirements. Current training initiatives have sought new and different ways to train potential students. In the USAR, any new member of a Reserve Command on the network receives user training. This training focuses on IA, to instill early on in the Service member's tenure the importance of good IA procedures. This training is provided either in a classroom setting or in a distributed learning format. USAR also established a Level II certified Systems Administrator/Network Manager (SA/NM) security course. Completion of this course is mandatory for all systems administrators on the ARNet. The classroom is located at the Army Reserve Readiness Training Center (ARRTC), Ft. McCoy, Wisconsin. It is a mirror site for the SA/NM security course at Ft. Gordon, Georgia. Each facility uses two classrooms and two sets of computers to train the UNIX/Solaris and Windows NT systems. The combined efforts of the USAR CIO staff and the ARRTC staff resulted in a flexible solution that also allows the training to take place in a single classroom with a single set of computers. These cost savings made it possible to enable a greater number of students to attend this training. To date, 284 Army Reserve, civilian, and contractor personnel have been trained at the ARRTC course.

USAR also initiated a Computer Network Defense (CND) course for senior administrators and members of the information operations community. This course is currently in development and will be certified at Level III. The first class is projected to begin in April 2001.

In support of general IA awareness, USAR held its annual Information Assurance Seminar in March 2000, attracting world-class speakers and military personnel, civilians, and contractors from all Army Components, other Federal Agencies, and the private sector. Each of the more than 250 attendees received a packet of IA training materials, including books, video tapes, and CDs for use in improving the IA training programs at their respective home stations. In addition, a five-day DoD Information Technology Security Certification and Accreditation Process (DITSCAP) course was established for USAR personnel. The course and the instructors were certified by DISA. This course used a collaborative environment to provide practical exercises in the application of DITSCAP.

The shortage of network security personnel is an ongoing challenge. A growing number of malicious activity incidents against Army networks mandate increased security requirements. These requirements have been levied on USAR Commands and installations with no additional network personnel staffing. The shortage of network security personnel has been identified as a shortfall and it has been validated through the budget process.



Soldiers pull a camoflauge net over a five ton truck at a remote radar site in Bosnia.

The Director of Command, Control, Communications, and Computers (DISC4) directed the implementation of the Network Security Improvement Program (NSIP). This program mandated the closing of holes in the network that allow unauthorized access to the ARNet and the installation of Intrusion Detection Systems (IDSs) and secure routers at all Nonsecure Internet Protocol Router Network (NIPRNET) and Secure Internet Protocol Router Network (SIPRNET) connections. The USAR has successfully completed Phase I, "Perimeter Defense" of the ARNet, and is now ahead of schedule in the completion of Phase II.

To protect the information that resides on its enterprise network, the USAR has applied several network security applications and technologies, including firewalls, intrusion detection systems, demilitarized zones, Internet caching, and other IA tools that are discussed further below.

As part of Phase II of the Army's NSIP, the USAR has implemented the Defense in Depth strategy across the ARNet by requiring that standard firewalls be installed at all USAR points of presence to the NIPRNET. Nineteen firewalls have been centrally procured and are being installed. Approximately 40 percent of the firewall implementation has been completed. The 7th Army Reserve Command (ARCOM) and 9th Regional Support Command (RSC) will become part of the ARNet once the firewalls at these locations are installed. These firewalls provide the USAR with Virtual Private Network (VPN) capabilities for the enterprise. Intrusion Detection Systems (IDSs) are currently fielded across the ARNet enterprise at all NIPRNET and NIPRNET connections. The IDSs are monitored by the ANSOC at Ft. Huachuca. Intrusion detection is done in accordance with ANSOC. ANSOC will begin monitoring all IDS points in the ARNet in FY 2001.

The Demilitarized Zone (DMZ) concept adapts firewall technology to provide on the Internet a secure zone for housing private servers. The DMZ sits between the Internet and an internal network's line of defense and contains devices accessible to Internet traffic, such as web servers, FTP servers, e-mail servers, and Domain Name Service (DNS) servers. The implementation of the firewalls and IDS software has allowed the creation of a DMZ at each portal from the ARNet to the NIPRNET and has provided another layer of protection for USAR information.

Twenty Internet caching appliances have been centrally purchased and are being installed across the ARNet at each NIPRNET point of presence on the enterprise. These appliances will improve throughput, maximize bandwidth, and reduce Internet response time, while providing the control and security required for this mission-critical network.

The DA has approved the Army Reserve Protected DNS architecture. The USAR has initiated for the network a new domain, known as USAR.Army.Mil. The DNS on the firewall is configured as a caching-only server, which "forwards only" to the Tier 1 DNS. The firewall is configured to block all external queries. COTS products are used to monitor the entire ARNet enterprise and notify Network Operations personnel in Atlanta of problems detected on all devices connected to the network. All routers on the network are password-protected, and passwords are changed at random intervals as personnel changes occur. Border routers at NIPRNET access locations contain access control lists in accordance with Army Computer Emergency Response Team (ACERT) guidelines. The USAR has plans to place Hot Standby Router Protocol (HSRP) routers at all Regional Support Command (RSC) locations to balance the data in and out of the RSC and avoid redundancy.

Army National Guard

The Army National Guard (ARNG) installed firewalls and IDSs for the purpose of securing front and back doors on the network. The ARNG secured funds to purchase links into the DISA hubs. The ARNG is increasing its involvement in the IA training arena, and IA Level I can now be completed on the website. The state of Vermont has taken the lead in the IO/IA environment and established an IO/IA training facility, which is considered a Level III certification for ARNG CERT. The ARNG is continuing to increase CERT team numbers in the states and to build experience and cohesiveness on the existing teams. The ARNG has 25 states; National Guard Bureau (NGB) and the Virginia Data Processing Unit have all established CERT teams for a total of 29 teams. Eight of the teams are at 100 percent staffing, and four teams are at 100 percent certification. The NGB CERT has been recognized as a Major Command CERT.

The State of Arkansas at the ARNG Professional Education Center has established a Systems Administrator (SA)/Network Manager (NM) Security Course Level 2 certification, as identified by the IA training structure. It is identical to the SA course offered at Fort Gordon, Georgia. The first class graduated in September 2000. Arkansas is using DoD/DA antivirus and web page security measures. Implementations of IAVA compliance reporting and registration of ARNG POCs on an ACERT list server are online at the GUARDnet and Army IA web page. COMSEC custodian and command inspector training, IAO/IAM training, and ARNG IA awareness training for users and information systems monitoring awareness training can be completed using web-based tools at the Signal Center at Fort Gordon, Georgia. ARNG also developed a web page for the dissemination of IA information.

Air National Guard

The Air National Guard (ANG) is an active partner of the Active Duty Air Force. ANG participates in all IA meetings, initiatives, brainstorming sessions, and strategic planning sessions as part of the total force. ANG is currently implementing a six-site Regional Operations and Security Center (ROSC) concept. This implementation will allow the ANG to more effectively use scarce IA resources. Using the AF suite of Network Management System/Base Information Protection (NMS/BIP) tools, personnel at the six ROSCs will be able to perform security testing, evaluation, and auditing at the subordinate units that they support. Because of minimal staffing at each base, this was determined to be the most effective method of providing these services to ANG units. A suite of NMS/BIP tools is also being installed at the ANG NOSC. Most significantly, in the standing up of the ROSCs, ANG was working with the Air Force Computer Emergency Response Team (AFCERT) to install Automated Security Incident Measurement (ASIM) intrusion detection equipment at these six ROSCs, which, for the first time, will provide intrusion detection capability to all ANG units.

ANG is actively engaged in increasing the security of ANG web pages. In addition, the Joint Web Risk Assessment Cell (JWRAC) is primarily composed of Reserve Force personnel, with two active duty members. This cell searches DoD websites, looking for possible security problems or breaches, as well as identifying information that should not be displayed on public web pages. The JWRAC thus provides support to all DoD agencies in this vulnerability assessment area.

In an effort to promote virus-free environments, ANG mandated the use of the most current DoD site-licensed, antiviral software. This was procured on the DoD site license by DISA. Regarding advisories, bulletins, and advisor y compliance messages, ANG follows AFCERT guidance and direction.

Marine Forces Reserve

Marine Forces Reserve (MARFORRES), located in New Orleans, Louisiana, is the Headquarters Command for all Marine Reservists and Reserve units located throughout the United States. An active duty Major General commands MARFORRES. The MARFORRES staff provides policy, guidance, direction, and support to 104,000 Reserve Marines across the United States.

Since its establishment by law in 1916, the Reserve of the United States Marine Corps has been responsible for providing trained units and qualified individuals to be mobilized for active duty in time of war, national emergency, or contingency operations. Serving with great distinction for the past 81 years, in every climate and place, Reserve Marines have regularly operated alongside the Active Component in the two World Wars, Korea, Vietnam, Desert Shield/Storm, and several other conflicts.

Over those years, the structure of the Marine Corps Reserve has evolved from small replacement units to major combat Commands.

Two of these Commands, 4th MARDIV and 4th MAW, have been colocated in New Orleans since 1977, but were not unified under a single Commander until 1992. Built around the nucleus Reserve staffs of the Division and the Wing and incorporating the FSSG and MCRSC, this new Command was designed to be a single cohesive structure, reflecting the "Total Force" principles and guidelines set forth by the Secretary of Defense in 1990. In 1994, the new parent Command was named Marine Forces Reserve. This designation established its parity with Marine Forces Pacific and Marine Forces Atlantic, the other two senior organizational entities making up the Fleet Marine Force.

In 1995, the Marine Forces Reserve Data Network (RNET) was established to link the 187 geographically separate Reserve Centers with the Headquarters in New Orleans. The primary computer center is located in New Orleans. The backup computer center is located in Kansas City. The RNET is the single largest data network in the Marine Corps Enterprise Network (MCEN).

From 1995 to 1998, RNET support was outsourced to a contractor. Currently, RNET is operated by the MARFORRES Assistant Chief of Staff, G-6 (AC/S, G-6). Immediately upon taking control of the network, the Marines of the AC/S, G-6 began improving the security, availability, and fault tolerance of RNET.

During the period from January 1999 to May 2000, the RNET was transformed through the following events:

- The two commercial Internet connections to RNET were terminated (January 1999).
- The MCEN was linked through the installation of an MCEN-operated firewall and IDS (February 1999).
- The number of network servers was reduced from 300 to 130.
- Network resources and administration were centralized to increase control.
- The network went from 215 Windows NT domains to a single NT domain.
- Network integration at 87 Navy/Marine Corps Reserve centers is underway.

Once the RNET infrastructure was updated, the focus was shifted to improving network operations. In support of this effort, MARFORRES initiated a contract to provide assistance in consolidating DITSCAP documentation. Contractors with a depth of knowledge in DITSCAP documentation are expected to be on site from October through December 2000.

Because of the nationwide dispersion of MARFORRES, distance learning is the focus of IA training. In fact, the first application of distance learning on RNET was an online training course designed to meet an end-user IA training requirement. There are plans to expand the use of distance learning to achieve IA training goals for system administrators.

Adopting the MCEN firewall greatly reduced the need for full-time RNET security personnel. The MCEN security team in Quantico, Virginia, provides "24x7x365" monitoring of the firewall and intrusion detection system. In addition to the existing RNET IA officer, an on-site contractor will be hired in January 2001 to maintain the DITSCAP documentation package, providing that funds are available for the position.

To protect RNET, the Marine Corps has applied several network security applications and technologies, including firewalls, VPNs, IDSs, and other IA tools. The MCEN firewall was installed in February 1999. The firewall was upgraded in April 2000. This is a sophisticated three-server system that provides very high throughput and availability. The firewall system is professionally administered, along with 30 other MCEN firewalls, from a network control center in Quantico, Virginia.

In support of the VPN, RNET uses the COTS MCEN-standard VPN system. The initial application is to support secure connectivity for the 12 Reserve Flag Officers. Use of VPN technology is expected to increase in the near future with the large number of Reservists connecting to RNET from home. An IDS is installed and operational and will be significantly upgrade in the near future.

The firewall contains a local DMZ, a protected area for use by the web server. The MARFORRES web server is the only device in the DMZ. Six high-performance proxy servers provide Internet content caching and inappropriate-site blocking for RNET. As part of the network modernization effort, the DNS services were centralized at New Orleans and Kansas City. Two specialized network appliances (rather than a number of COTS servers) provide DNS for RNET. These devices are called IP servers and are configured to provide automatic fail-over of this critical network service.

LAW ENFORCEMENT/ COUNTERINTELLIGENCE LIAISON

Law Enforcement (LE) and Counterintelligence (CI) provide critical support to the Department's IA Defense in Depth. The LE/CI community usually provides the initial response to a criminal, terrorist, or counterintelligence attack on our DoD systems. Using search warrants, subpoenas, and consensual and nonconsensual wiretaps and interviewing witnesses and informants, it must first establish the origin of the attack. Once that is established, senior executives can step in and determine a course of action.

Active and aggressive preventive action can also be taken to deter attacks before they occur. In FY 2000, LE/CI have taken several significant steps to better provide this critical support for IA. Chief among these are the creation of a Law Enforcement and Counterintelligence Center for Computer Network Defense, the establishment of a Computer Network Defense Operations Chiefs Working Group, the hosting of a DoD-wide computer crime workshop, and the establishment of a DoD Computer Forensics Laboratory (DCFL), in coordination with a Defense Computer Investigations Training Program. In addition to these activities, the crime investigators of the Air Force Office of Special Investigations provide rapid worldwide response to intrusions, and the Naval Criminal Investigative Service manages naval security programs for the Department of the Navy.

Law Enforcement and Counterintelligence Support to IA

Law Enforcement and Counterintelligence Center for Computer Network Defense

A DoD Directive currently in coordination establishes the Defense Criminal Investigative Organization's Law Enforcement and Counterintelligence Center (DCIO's LE&CI Center). An organization that coordinates LE and CI investigations and operations in support of CND, it is staffed by all Defense Criminal Investigative Organizations (DCIOs). This directive formalizes and institutionalizes the LE/CI Cell currently colocated with the JTF-CND.

With operational direction from the DCIOs, the LE&CI Center is to serve as the primary interface between DoD and the Federal Bureau of Investigation's (FBI's) National Infrastructure Protection Center (NIPC). It deals with CND-related law enforcement and counterintelligence issues and responds to the information requirements of the U.S. Space Command and Components. The Center coordinates and provides analytical services to CND investigations and operations among the DCIOs and the Common Operating Picture (COP).

The Center also coordinates CND-related investigations and operations across DoD Components or Federal Departments/Agencies and provides law enforcement- and counterintelligence-generated information to a

CND COP. All DCIOs exchange CND-related information with the LE&CI Center. The LE&CI Center will maintain an information system to provide coordinated information to the CND COP and to support the operational needs of DCIOs.

Computer Network Defense—Operations Chiefs' Working Group (OCWG)

Recently, DoD has established the Computer Network Defense Operations Chiefs' Working Group (OCWG). Its purpose is to provide direction, guidance, and support to Defense Criminal and CI components and to the Joint LE&CI Center colocated with the JTF-CND.

The OCWG comprises the most-senior representatives responsible for the computer investigations and operations program within each of the DoD's Criminal Investigative and Counterintelligence Organizations, including the Air Force Office of Special Investigations (AFOSI), the Defense Criminal Investigative Service (DCIS), the Naval Criminal Investigative Service (NCIS), the U.S. Army Criminal Investigation Command (USACIDC), and the U.S. Army Office of the Deputy Chief of Staff for Intelligence (ODCSINT).

Associate membership in the OCWG, to be expanded as needed, will include the Defense Computer Forensics Laboratory (DCFL), the Defense Computer Investigations Training Program (DCITP), the Defense Component Computer Network Defense LE&CI Center, and the DIAP-LE/CI Coordinator.

DoD-wide Computer Crime Workshop

In May 2000, the LE/CI liaison element of DIAP sponsored a Computer Crime Workshop in Colorado Springs, Colorado. This three-and-a-half-day workshop, which focused on the response to cyberincidents, was held at no cost to DoD, except for the temporary duty travel costs of attending personnel.

The workshop had several objectives, including establishing trained "go-to" computer crime response teams at each installation/organization and providing baseline education and awareness for the members of each team. In addition, it provided current legal guidance on computer forensics, search and seizure, and the monitoring of DoD computer systems and a certain degree of technical awareness to agents and attorneys.

Beyond this scope, the workshop aimed at providing all participants with current DoD-wide guidance on intrusions and computer crime, making key DoD personnel aware of new organizations and programs such as DIAP, JTF-CND, NIPC, CIAO, DCFL, and DCITP and providing a network of contacts for assistance within the DoD.

The audience represented individuals from each DoD installation or organization who would be involved in every computer crime investigation.

Key positions included Information Assurance Officers, Criminal Investigators, and Judge Advocate Generals and Attorneys. Approximately 310 DoD personnel attended the entire workshop, and another 20 or so individuals from the local Colorado Springs area attended sessions that specifically interested them. Participants came from all over the world, representing approximately 60 organizations from 28 states, as well as Europe and Pacific regions. Figure 5 shows the work demographics of the participants, and Figure 6 their Components within DoD.

Feedback was overwhelmingly in favor of an annual Computer Crime Workshop. The next one is tentatively scheduled for late April or early May 2001.

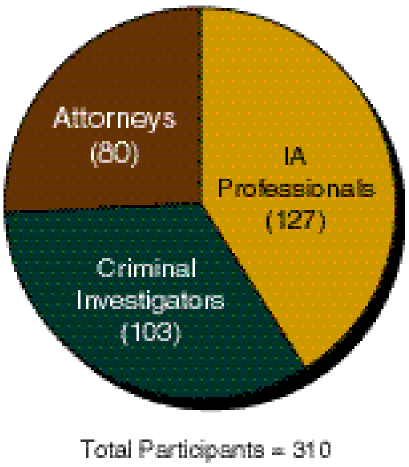


Figure 5

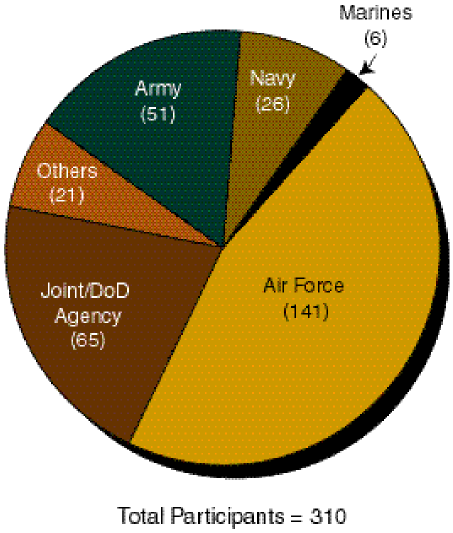


Figure 6

Defense Computer Investigations Training Program

Based on decisions made by the Director of Counterintelligence for OASD (C3I), the Air Force led the way to the development of the Defense Computer Investigations Training Program (DCIPT). The mission of the DCITP is "to provide computer investigation training (CIT) to individuals and DoD elements that must ensure Defense information systems are secure from unauthorized use, counterintelligence, and criminal and fraudulent activities." DCITP is the only government facility specifically and singularly dedicated to the development and delivery of computer investigation training. The multigovernment agency and contractor staff (see Figure 7 for organizational chart) provides to DCITP students a rigorous, thorough training in the disciplines that constitute the curriculum, delivered by highly experienced and committed instructors.

DCITP has annually conducted a needs assessments process that allows it to stay current with training needs and requirements. Accordingly, DCITP is in the process of developing other courses such as Operating System (OS)-specific courses for intrusion and forensic examinations,

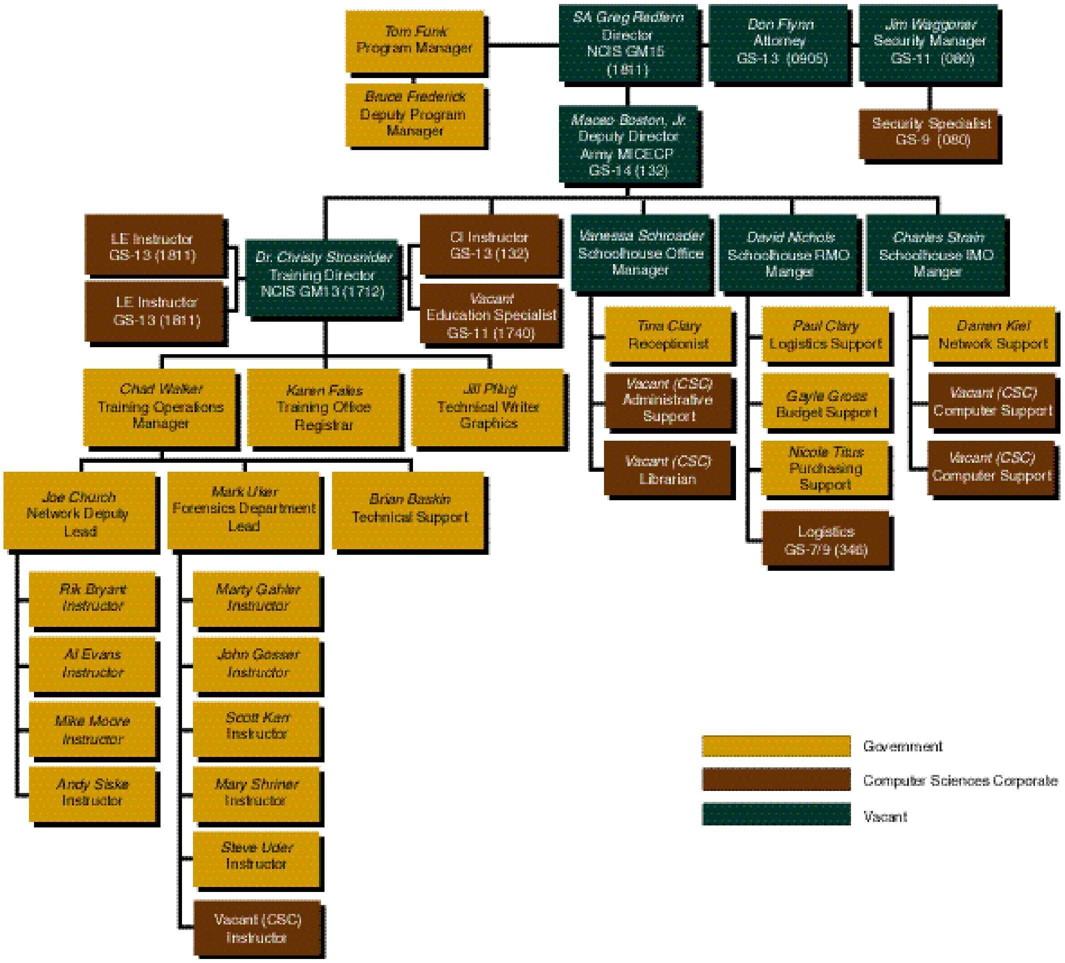


Figure 7

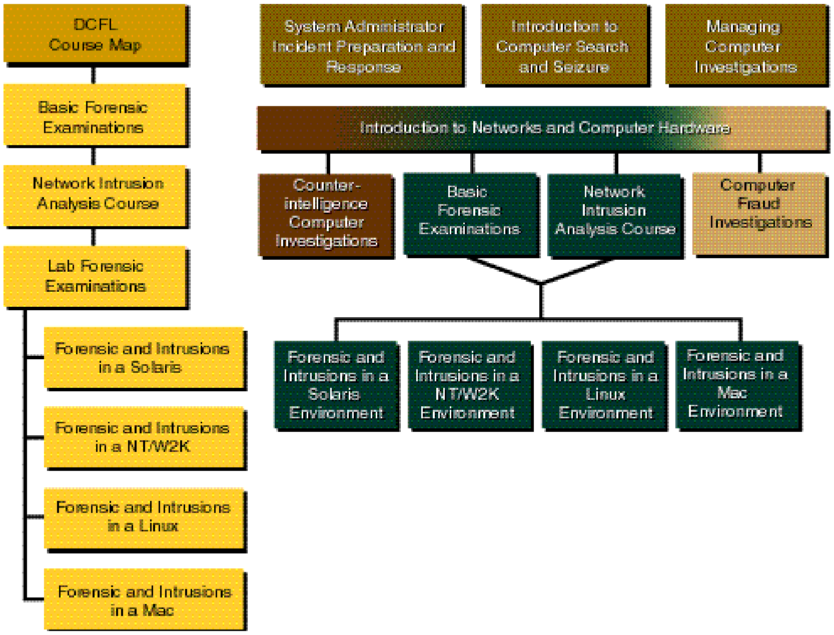

DCFL Course Map
Basic Forensic Examinations
Network Intrusion Analysis Course
Lab Forensic Examinations
Forensic and Intrusions in a Solaris
Forensic and Intrusions in a NT/W2K
Forensic and Intrusions in a Linux
Forensic and Intrusions in a Mac
System Administrator Incident Preparation and Response
Introduction to Computer Search and Seizure
Managing Computer Investigations
Introduction to Networks and Computer Hardware
Counter-intelligence Computer Investigations
Basic Forensic Examinations
Network Intrusion Analysis Course
Computer Fraud Investigations
Forensic and Intrusions in a Solaris Environment
Forensic and Intrusions in a NT/W2K Environment
Forensic and Intrusions in a Linux Environment
Forensic and Intrusions in a Mac Environment

Figure 8

Counterintelligence Computer Investigations (CICI), Computer Fraud Investigations (CFI), and Managing Computer Investigations (MCI). The current DCITP course map is Figure (8).

DoD Computer Forensics Lab (DCFL)

The mission of the DoD Computer Forensics Lab (DCFL) is to provide digital evidence processing, analysis, and diagnostics for DoD counterintelligence, criminal and fraud investigations, operations, and programs. In order to fulfill this mission, DCFL also performs other functions: setting DoD standards for forensic analysis of digital evidence; developing and managing DoD's forensic media analysis research and development projects; and conducting liaison with counterpart law enforcement, computer security, and intelligence agencies.

On 10 February 1998, the Deputy Secretary of Defense signed the Defense Reform Initiative Directive (DRID) No. 27 that directed the Air Force to establish the DCFL. Now, two years later, the DCFL is housed in its permanent facility in Linthicum, Maryland. The facility is operational, and most of the staff is in place and performs casework. For the last two fiscal years, the program has been managed to budget, met its initial implementation goals, and is ready to take on additional missions if required to do so by the DoD.

During the time that this facility was being constructed and the staff hired, the DCFL processed 108 cases. Almost half of these cases were critical, involving foreign or important computer intrusions, espionage, death, or sensitive counterintelligence matters.

DCFL Support to Information Assurance

The DCFL supports IA as a reactionary element to an incident, not one that will detect or defend against intrusion. Following requests for analysis from LE, the DCFL performs forensic analysis of intrusion cases. Results are sent to the requesting agent, who can use them to trace the attack back to the source, identify the suspect, and prosecute.

Typically, a case will generate several reports: the first is based on the victim system, the next is of logs from firewalls and/or phone logs, and the last is hopefully from the suspect's computer. All this information is coordinated to create a picture of the intruder and the timeline of the events.

What makes the reports particularly useful is that they can be used in court. DCFL has put in place evidence-handling procedures that make it possible to use the reports in a number of ways: First, they can be used to obtain search warrants and subpoenas—these are the tools that LE uses to track back to the attacker and to collect evidence for prosecution. Second, the prosecutor uses these reports to build a case against the subject of the investigation.

Intrusion cases are complex cases that take longer to complete than most other cases. They also require that the analyst have special experience and training. Figure 9 indicates the progress made in reducing the average time that it takes to complete a case. For the information to be of any use to an investigator, it must be fresh; therefore, these time frames have to be reduced still further. This is being worked upon by automating more functions. Two R&D projects are currently aimed at reducing the average time required to complete a case: The first is a partnership of DCFL with MITRE Corporation and Rome Laboratory in the development of a product called the Forensic Intrusion Analysis Tool (FIAT). Case agents will use FIAT to gather intrusion information from victim systems. The second project, called Starlight, is a data-mining tool that helps conduct link analysis in a collaborative effort with Pacific Northwest Laboratory, a DoE laboratory. In these two instances, DCFL is partially funding the work to ensure that it is responsive to DCFL's needs. The integration of these new tools will streamline and automate processes, thus reducing the overall timelines.

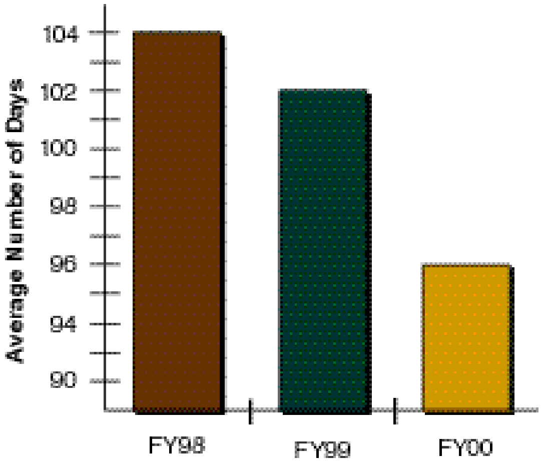


Figure 9

Support to LE/CI

DCFL accepts all case types from DoD LE/CI. It has supported a major seizure of evidence and a number of counterintelligence operations for the Air Force. In addition, Army Military Intelligence has requested DCFL support in reviewing its procedures related to computer systems and counterintelligence operations.

The caseload has climbed quickly since FY 1999 Q2, when the lab began accepting all case types. Before then, the lab only accepted high-priority cases: those involving foreign or critical computer intrusions, espionage, death, or sensitive counterintelligence matters. As Figure 10 shows, the number of cases has grown considerably. Two factors will make the caseload continue to grow: (1) an even inflow of cases from all Services and (2) training agents in the Services to look for digital evidence. Both of these are taking place now, with the diversity of case sources a short-term issue and training a long-term one.

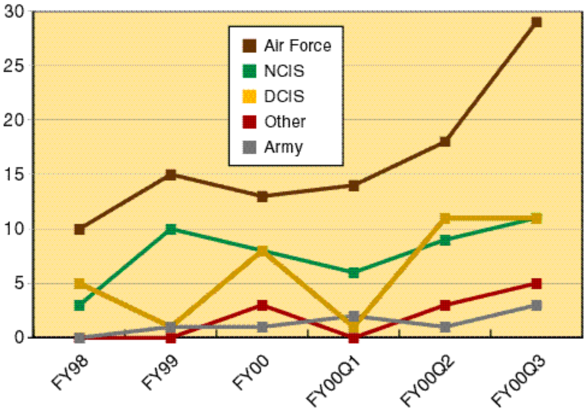


Figure 10

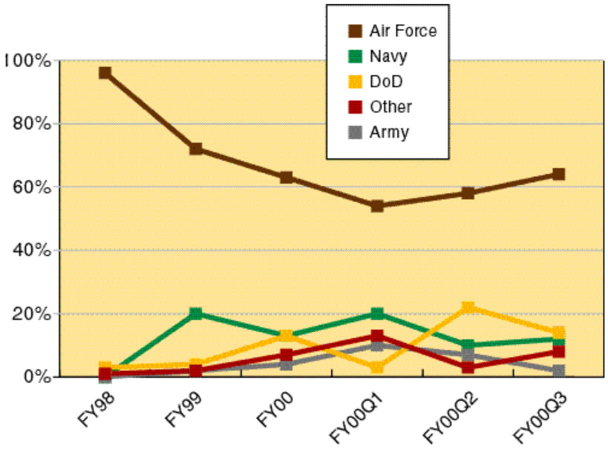


Figure 11

Over the past few quarters, the list of case sources has become much more diverse, as Figure 12 indicates. Although the Air Force still accounts for more than half the lab's business, this should change over time as more investigators in other Services are trained to look for digital evidence and as full participation of all Services is realized.

Cases reaching DCFL fall into one of three categories: Category I includes those involving foreign or critical intrusions, espionage, death, and sensitive counterintelligence matters. Category II includes all other intrusions and significant counterintelligence, sexual assault, major fraud, and major narcotics investigations. Category III

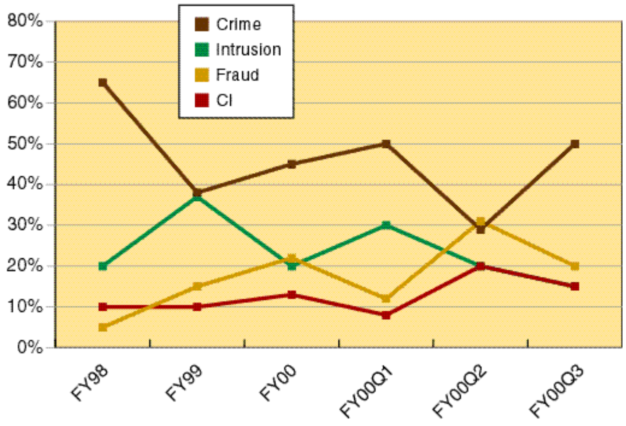


Figure 12

involves all other remaining case types. Figure 13 shows the distribution of case categories closed by DCFL. There is a downward trend for high-priority cases worked at the DCFL; their number has not gone down, but rather the number of lower-priority cases has increased.

DCFL recently assisted Defense Criminal Investigative Service (DCIS) with on-site support for a major search and seizure of digital evidence at the subject company's headquarters. This was the largest of 25 sites and the most likely to have the evidence that DCIS was searching for. DCFL personnel imaged 12 servers and more than 160 workstations. The company had in place a control for an environmentally sensitive system, making the handling of the case extremely sensitive ecologically and forensically. Fourteen deployed personnel accomplished the mission in three days.

DCFL's Engineering Branch has provided support to the counterintelligence community, either directly or through a set of procedures. It is currently supporting three operations for the Air Force Office of Special Investigations (OSI) and has opened the door to other Agencies with similar support. It is reviewing procedures for the Army Military Intelligence (MI).

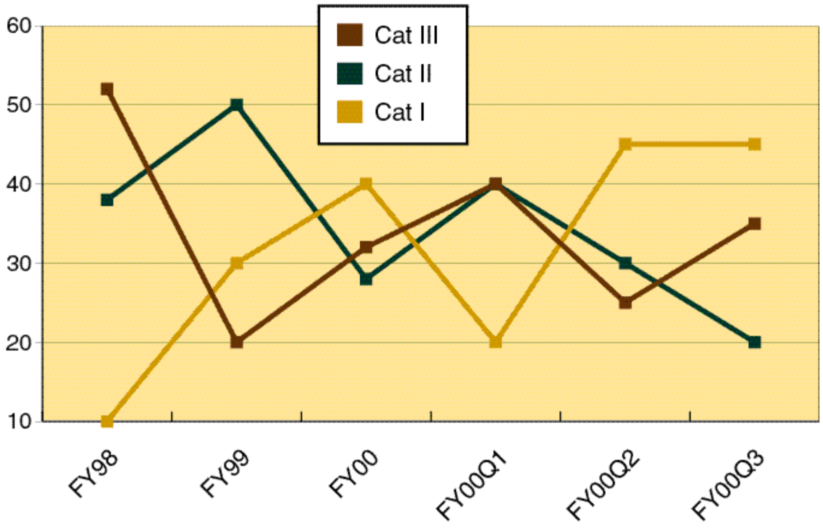


Figure 13

Moreover, DCFL can provide computer professionals with the appropriate clearances, which speeds up the process for any DoD activity seeking assistance. DCFL's Engineering Branch is working with the National Aeronautics and Space Administration (NASA) to complete a Forensic Tool Suite—a set of forensic tools that will reduce the amount of analysis time required to complete a case. The goal is to provide the forensic analysts with a platform that can work with multiple file systems. When completed, the tools will allow analysts to examine 13 different file systems, including Windows 95/98, Windows NT, Mac, Sun, and a number of other UNIX systems. Along with caseload and timeliness, the DCFL can thus give DoD LE/CI the technology edge needed in the present environment.

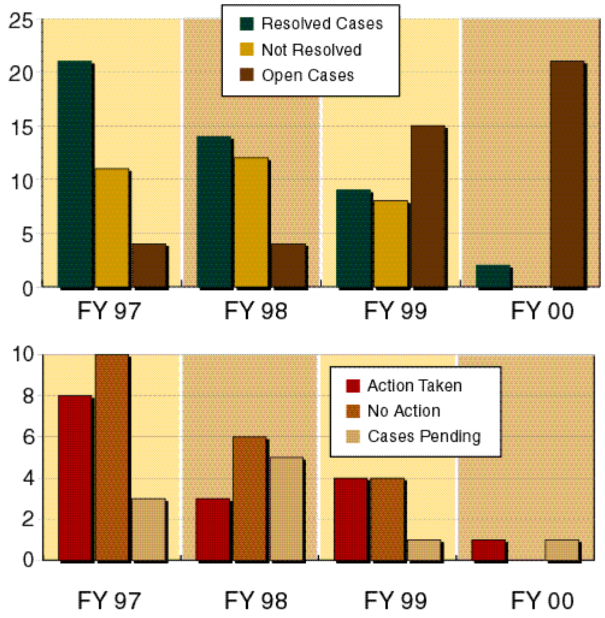


Figure 14

The DCFL and DCITP are great government success stories. First-rate organizations in terms of costs, efficiency, and performance, they have received recognition on the national and international level for their professionalism and capabilities and fill an important role in the DoD's IA efforts.

Air Force Office of Special Investigations (XOSI)—Computer Investigations and Operations Branch

Air Force computer crime investigators (CCI) have had a busy year, conducting several successful and highly visible intrusion investigations, providing real-world support to the warfighter, and conducting the first online undercover operation. By the end of the Kosovo conflict, 12 OSI CCIs (25 percent of the CCI program) had deployed in support of this operation.

To date, the intruder was identified in 53 percent of the computer crime cases—including still open ones—in a total of 60 cases. Of these, 24 cases involved members of the military, 11 were foreign individuals, and 25 were U.S. civilians. Cases with overseas connections are increasingly prevalent—making it more difficult to identify the intruder because of the length of time and coordination it takes to gather information.

Army Criminal Investigation Command

Computer Crime Investigation Unit

The Computer Crime Investigation Unit (CCIU) has worldwide responsibility for investigating intrusions into Army interest computer networks to support and enhance the Army Information Assurance Program. The CCIU works closely with Army network management organizations in support of critical infrastructure protection/information assurance, and provides direct support to DoD and other Federal agencies in joint computer crime investigations. The CCIU maintains a core of highly trained, experienced special agents with appropriate technical capabilities, clearances and access to conduct investigations involving computer intrusions. These special agents conduct sensitive and classified computer crime investigations, conduct forensic examinations of computer hardware and media in support of their computer crime investigations and conduct crime prevention surveys in the form of computer crime vulnerability assessments (CCVAs) of Army networks. The CCIU maintains criminal intelligence on computer-related issues and serves as the primary focal point for the Army Computer Emergency Response Team (CERT) community to report network intrusions. In addition, the CCIU provides a liaison officer to the Land Information Warfare Activity (LIWA). The CCIU provides technical assistance to worldwide CID elements investigating computer-related crimes.

Both the CCIU and CID field elements are augmented in the investigation of computer intrusions and computer related crime by the forensic abilities of the U.S Army Criminal Investigation Laboratory (USACIL). The USACIL is a USACIDC major subordinate command that provides multi-disciplinary forensic laboratory services to the DoD and other federal agencies. The USACIL provides quality and timely, state-of-the-art forensic laboratory support. It also provides on-site scene support to help in processing crime scenes beyond the capability of the requester and providing guidance to investigators.

Significant Investigations

Following are examples of CCIU investigations and associated outcomes. During June 1999 an Army web page hosted on a Pentagon network was altered. A 20-year old civilian from Green Bay, Wisconsin was identified as a suspect. Forensic analysis of his computer produced evidence that he had committed the intrusion. During March 2000 the perpetrator pled guilty in Federal District Court and was sentenced to 6 months imprisonment, $8,054.00 in restitution, and 3 years of supervised computer and telephone access.

During September 1999, the United States Army Enlisted Records and Evaluation Center, Indianapolis, IN (USARERC) reported problems with their network. Analysis of their computers by CCIU that revealed an exploit called Back Orifice 2000, a remote system administration tool used on Microsoft 95, 98 and NT networks, had been installed. Ten computers were infected; 58,000 files were deleted from the file server. The investigation revealed that an Army Private First Class (E-3) was the intruder. Forensic examination of the soldier's home computer produced evidence to substantiate the offense. The soldier was court martialed, found guilty and sentenced to a reduction in grade to Private (E-1), forfeiture of all pay and allowances, 4 months confinement, and a Bad Conduct Discharge.

Department of Defense Inspector General

The Defense Criminal Investigative Service

The Defense Criminal Investigative Service (DCIS), in line with the DoD criminal investigative organizations (DCIO), is focused on the investigation of computer crimes in order to implement the Defense in Depth Strategy. To meet this challenge, DCIS has placed agents trained in computer intrusion and forensic analysis in each of their six field offices, which are located throughout the US. As a result of this effort, DCIS has trained and equipped over 20% of its agent corps in computer intrusion and/or forensic analysis investigative techniques. The computer hardware and software procured for use in computer crime investigations has been extensively utilized in the execution of search warrants, forensic analysis of evidence, evaluation of system vulnerabilities, and use during the covert portion of undercover investigations.

An intensive training program for the computer crimes special agents has been obtained from a variety of sources including private contractors, the Federal Bureau of Investigation (FBI), the Federal Law Enforcement Training Center, and the DCITP. The DCITP will continue to be the major source of training for the DCIS computer crimes special agents providing courses from the basic to advanced training programs.

In order to coordinate DCIS computer crimes investigations, DCIS is directly connected to the LECIC within the JTF-CND, through the full time DCIS LECIC representative. DCIS also has a full time senior special agent assigned to the NIPC that is located at FBI Headquarters.

During FY2000 DCIS actively worked 89 computer crimes cases involving web page defacements, child pornography, theft of technology, computer intrusions, and virus attacks. These cases resulted in 6 arrests, the execution of 13 search warrants, and the indictment of 13 individuals.

Naval Criminal Investigative Service

The Naval Criminal Investigative Service (NCIS) is a worldwide organization responsible for providing counterintelligence support, conducting criminal investigations, and managing naval security programs for the Department of the Navy (DON).

Unique to the DON Information Infrastructure Protection mission is the NCIS Computer Investigations and Operations (CIO) Department. The CIO integrates and analyzes CI and Law Enforcement information to enhance the protection of DON personnel, technologies and facilities. CIO focuses on five threat areas: hackers, criminal groups, foreign intelligence services, terrorists and insiders. CIO supports NCIS criminal and counterintelligence missions, the DOD Critical Infrastructure Plan, and Presidential Decision Directive 63.

During the past calendar year the NCIS has opened 99 intrusion investigations as a result of criminal elements targeting U.S. Navy Sites. During this same period NCIS generated 54 Operations Reports (NOR) reporting intrusion and/or related computer incidents. NCIS currently has three undercover operations and 16 infrastructure protection operations ongoing. NCIS has closed 71 intrusion investigations during Fiscal Year 2000.

Services

ARMY

During FY 2000, the Army significantly expanded the scope of its IA efforts to include a number of important new initiatives under the Network Security Improvement Program (NSIP). It substantially increased the amount of IA security tools/technologies throughout its information systems and network infrastructure. The Army also integrated network security initiatives and emerging security technologies into the architectures of the Digitized Division/Corps and the Interim Brigade Combat Team (IBCT). Significantly, in recognition of its leadership in the area of biometrics, the Department of Defense appointed the Army as Executive Agent for the DoD program, so that the Army is chartered to lead, consolidate, and coordinate all biometrics IA activities for DoD.

The NSIP is the Army's strategy for implementing the DoD concept of Defense in Depth, in accordance with DoD policy and guidance for implementing Information Assurance (IA) and Computer Network Defense (CND). The NSIP is a comprehensive set of innovative policies and procedures, state-of-the-art IA hardware/software-enabling technologies, an active training program, and retention initiatives. It is designed to counter ever-expanding asymmetric threats directed toward Army information systems and networks, from the sustaining base to the deployed force, across the full spectrum of conflict. The NSIP integrates IA security solutions into the Army's command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architectures under the Protection Plan for Army Tactical Information Systems.

In the Forefront of IA

To defend the networks and enclaves through Defense in Depth, there has been a considerable increase in the density of systems and network security tools and technologies layered throughout the Army portion of the Defense Information Systems Network (DISN). In addition to the hundreds of firewalls and intrusion detection systems (IDSs) purchased by local commanders, the Army has centrally purchased and fielded more than 900 firewalls, security routers, and proxy technologies and 2,500 IDSs to strengthen the infrastructure. In concert with these actions, the Army sought to centrally control, through the procurement and maintenance process, the quality of IA tools and licenses for Armywide use of firewalls and firewall-like technologies, IDSs, and proxy technologies.

To ensure that IA tools are of uniform quality, the Army established an operational policy that the only IA tools authorized for use on Army systems and networks are those listed on the Army IA Blanket Purchase Agreement (BPA). Thus a new tool cannot be introduced into the IA architecture unless it meets the minimum quality specifications required by the IA BPA. For example, all existing tools must meet Common Criteria Evaluation Assurance Level

(EAL) 2 and EAL 3 by 31 December 2000. Waivers for the use of tools other than those on the IA BPA must be approved by the Office of the Secretary of the Army's Director of Information Systems for Command, Control, Communications, and Computers (ODISC4).

The Army is also in the forefront in verifying that the DoD's Information Assurance Vulnerability Alert (IAVA) "positive control" process is being fully implemented. The Army created and dispatches an IAVA Compliance Verification Team (CVT) to conduct short-notice, on-site inspections of units that have been randomly selected Armywide and to determine whether they have fixed vulnerabilities identified in IAVA messages. The CVT comprises security technicians and Army Criminal Investigation and Army Audit Agency personnel, who not only inspect but also provide on-site support, assistance, and recommendations for improving security. The IAVA CVT has inspected more than 25 units worldwide, and its findings require a reply by endorsement to the Army Chief Information Officer (CIO) on follow-up action. Results are also provided to the Senior Army Leadership, as required. The presence of the IAVA CVT and the knowledge that the Army's Senior Leadership is actively involved in reviewing the findings have proven together to be a most valuable tool in improving the security of Army systems and networks.

The NSIP includes a process for the identification of and elimination or protection from all Internet Service Providers (ISPs) and other back doors into the Army's portion of the DISN, as mandated by the Office of the Secretary of Defense (OSD) memorandum. In addition, the Army reengineered its Domain Name Service (DNS) security architecture worldwide. The DNS is the Army's "electronic address book," and the new security architecture protects it from tampering. From February to September 2000, the new security architecture has denied more than 2.8 million unauthorized queries for information from the electronic address book, more than 437,000 of which were from foreign sources.

A soldier from the First Armored Division assesses the situation in the field.

IA Training and Certification

One of the Army's biggest success stories is the acceleration of training and certification programs for Systems Administrators, Network Managers, Information Systems Security Officers/Managers, and user-level personnel. Training expansion and upgrades included development of intrusion detection system (IDS) and firewall training courses. Most significantly, Systems Administrator and Network Manager security training have been expanded from one laboratory with only 240 spaces in April 1998 to 12 laboratories with 2,760 spaces annually by the end of FY 2000. Every space has been filled and is projected to be through 2001.

Incidents such as the FBI investigation of "Moonlight Maze" (a series of intrusions into U.S. Government computers) and other related attacks on Army networks and systems highlighted the threat of a remote attacker being able to install a program to "sniff" the Internet Protocol (IP) packets, including user passwords, as they traverse the network. To counter this threat, the Army procured a proactive, security monitoring "antisniff" tool to scan networks and detect compromised machines. This software helps Army Computer Emergency Response Team (ACERT) personnel to remotely detect packet sniffing on addressable devices, regardless of the remote operating system.

NSIP is the driver behind accelerating the evaluation and integration of new and emerging technologies into the Defense in Depth strategy. Most notably, the Army has evaluated malicious mobile code detection and eradication tools. The Army conducted a market survey of third-party malicious mobile code detection software and has begun limited testing of two products. The Army has been a strong advocate of identifying and adopting DoD enterprisewide technical solutions to the malicious mobile code threat. The Military Communications Electronics Board (MCEB) has assigned the lead to the Army in testing the effectiveness of third-party malicious mobile code detection and eradication software.

IA in the Field

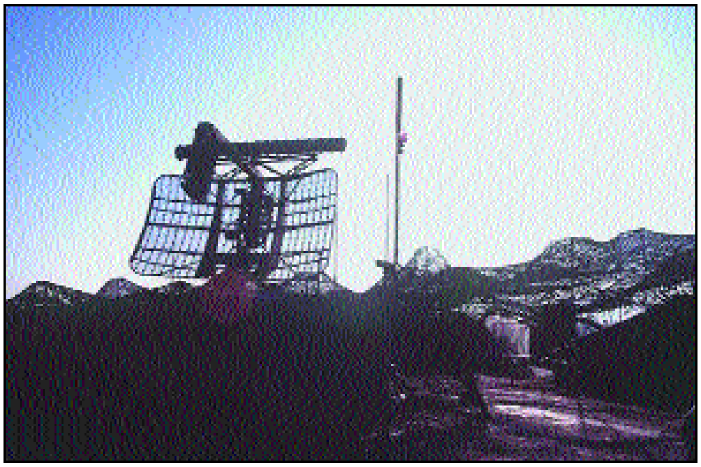
The Interim Brigade Combat Teams (IBCTs) and the Digitized Division/Corps both heavily incorporate IA into their operations. The Army updated the Protection Plan for Army Tactical Information Systems. This plan outlines requirements for security planning and vulnerability testing and identifies acquisition milestone decisions. It also provides, early in the acquisition or development process, a mechanism for review and feedback that enhances the integration of security mechanisms in the future force.

The first IBCT initiative extended the requirement for certification and accreditation (C&A) of automated information systems (AISs). This initiative will now encompass weapons platform AISs that were previously exempt from this requirement.

This was a logical evolution of existing policy, based upon the extension of connectivity down to the platform level under force digitization. The process of C&A has greatly enhanced system survivability through systematic security planning, as well as through identification and rectification of potential system vulnerabilities.

The First Digitized Division (FDD) fielded IA Defense in Depth capabilities that included perimeter-, network-, enclave-, and host-level IA tools, as well as new tactics, techniques, and procedures (TTPs). The Army conducted three major IA network assessments of the emerging IA architecture being fielded to the FDD. Each assessment provided critical feedback to the materiel developers on the effectiveness of the current architecture. Adjustments to the architecture, configurations of IA components, and TTPs were based upon previous findings and evaluated for effectiveness. These changes ensure enhanced capability and survivability.

A major step forward was the Army's transitioning of security software applications, developed by the Army Communications-Electronics Command (CECOM) from an Advanced Technology Demonstration (ATD), into operational use for the FDD. The tool, the Security Operations Suite (SOS), is a software application developed to simplify the use and configuration of Common Operating Environment (COE) security tools. As designed, the SOS can be expanded to support future tools, if needed. It presents to the user (administrator) an intuitive graphical user interface (GUI) for access to all functions provided by the IA tools. The SOS gives users the capability to configure these tools either from their own machines or from any other SOS-equipped machine on the network. Network communications between the remote user and host machine are protected against security attack through the use of both authentication and encryption. All messaging will be as short as possible to accommodate the low bandwidth environment of tactical radio links.



View of a TPN-19 Radar at the Radar Approach Control Center at Tuzla Air Base, Bosnia.

The FDD also conducted much needed system-level Information Operations Vulnerability/Survivability Assessments (IOVSAs) on many of its systems. This effort primarily focused on the Army Battle Command

System (ABCS) and its related network backbone systems. These IOVSAs identified in operating systems, applications, and system components vulnerabilities that could potentially be exploited. Providing the results of these IOVSAs to the materiel developer for rectification, mitigation, and determination of risk acceptability has significantly enhanced the overall survivability of the individual systems and reduced risks to the tactical networks.

Major Army efforts to defend the computing environment include Public Key Infrastructure (PKI) and biometrics initiatives. In support of DoD's PKI activities, the Army backs the common access card (CAC)/PKI and is actively involved in supporting the implementation timelines. Under PKI, the Army has issued certificates to implement encryption and to enhance security on more than 1,200 web servers restricted to the conduct of Army business, and the numbers increase daily.

Biometrics Efforts

Over the last two years, the Services have determined that the majority of break-ins and unauthorized penetrations to sustaining base information systems have occurred by subversion of passwords or user ID accesses that use alphanumeric passwords. Biometrics is defined as a measurable, physical characteristic used to recognize the identity, or verify the claimed identity of a person. The use of biometrics effectively eliminates the need for passwords or personal identification numbers (PIN) in favor of a unique, identifiable physical characteristic, for example, the shape of one's iris, voice characteristics or a fingerprint. Biometrics can enhance other security measures designed to combat unauthorized access through either password breakage or tactical overruns to DoD information systems.

The Army completed a biometrics feasibility assessment in January 2000 along with a social and legal study in February 2000. The results of the studies were reported to Congress in June 2000. Subsequently, the President signed Public Law 106-246 on July 13, 2000 naming the Army as the DoD Executive Agent, chartered to lead, consolidate, and coordinate all biometrics IA activities for the Department. The charter also includes a mandate to establish oversight and support infrastructure for all DoD biometrics programs.

As the Biometrics Executive Agent, the Army CIO established the Biometrics Management Office (BMO) in the Military District of Washington. The BMO is to serve as the coordination and development center over a full spectrum of biometrics systems and technologies. Effective use of biometrics will give the DoD a decisive edge in all operational environments, providing it with the best and most reliable security access control for information and weapons systems.

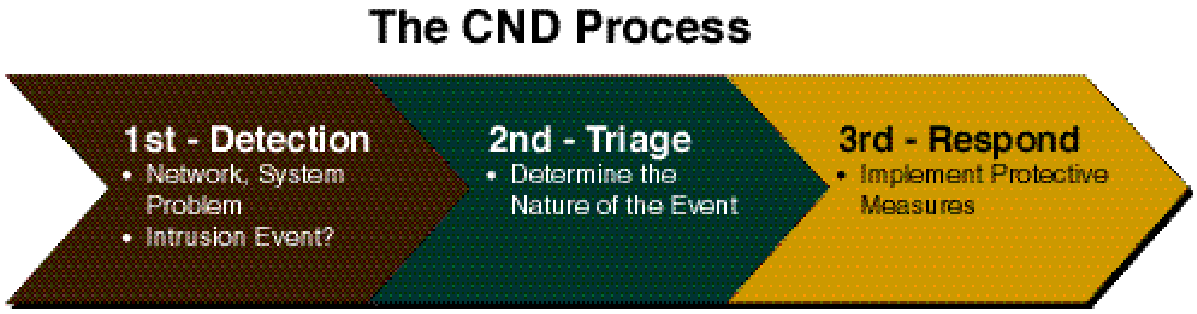

The CND Process
1st - Detection
• Network, System Problem
• Intrusion Event?
2nd - Triage
• Determine the Nature of the Event
3rd - Respond
• Implement Protective Measures

Figure 15.The CND Process at the Theater NOSCs and Regional CERTs

The BMO's primary mission will be to develop an acquisition-based strategy to deploy COTS biometrics applications. Fulfillment of this mission would ensure definitive access control to critical information and weapons systems in all environments. The Office also provides management expertise to leverage the experience and knowledge of the existing partnerships between industry and academia. In addition, the BMO will develop an implementation strategy for integrating biometrics into existing and planned Army information and weapons systems.

The BMO established the Biometrics Fusion Center in Bridgeport, West Virginia this fiscal year. The Fusion Center will assist the effort by becoming the primary = facility for the acquisition, testing, and oversight of Biometric products and will monitor pilot programs, as well as provide assessment/assistance teams to DoD partners. The Fusion center will also act as a repository for storing biometrics templates as a continuity of operations site.

Computer Network Defense

The heart of the Army's CND capability is the Army Computer Emergency Response Team (ACERT) and the Network Operations and Security Center (ANOSC). The Army's CERT and NOSC infrastructure is the best way to implement DoD guidance in terms of colocating CND operations with network management and ensuring full coordination of the two functions. While the ACERT Coordination Center is located at Ft. Belvoir, Virginia, and the Army NOSC is at Ft. Huachuca, Arizona, the workhorses of the CND infrastructure are the four regional CERTs and theater NOSCs colocated worldwide. Each regional CERT and colocated theater NOSC provides a mutually supportive "911" capability to Army users to sort through network outages and anomalies and identify and react to cyberattacks. These colocated regional CERT and theater NOSC centers are at Ft. Huachuca, Arizona; Mannheim, Germany; Ft. Shafter, Hawaii; and Camp Walker, Republic of Korea. The regional

CERTs and theater NOSCs work together to monitor IDSs installed at all Army gateways to the Nonsecure Internet Protocol Router Network (NIPRNET) and on critical servers. Together, they are the Army's capability to provide a fully coordinated Common Operational Picture (COP) of the health of the Army's systems and networks and to provide Attack Sensing and Warning (AS&W) support to Army users worldwide in protecting against, and responding to, cyberattacks.

The Armywide AS&W capability is accomplished at the Army Intelligence and Security Command's Information Dominance Center (IDC), which resides within the Land Information Warfare Activity (LIWA). The IDC houses state-of-the-art technology and tools to support collaborative planning, analysis, and execution of information operations (IO). Data from the Army's worldwide Defense in Depth sensor grid are shunted to the IDC, whose technical capacity to receive, store, and sort through terabytes of information, reduce data, and correlate events gives the Army a one-of-a-kind capability to accomplish the AS&W mission. The IDC reached initial operational capability on 01 October 2000 and is currently in Phase II of a three-phase development process. The IDC allows the Army to shift from an environment of information overload to information management, where more data equals better information and better decision making. The first of two primary IDC objectives is that the IDC will maintain information superiority while planning and executing military operations. The second of these primary objectives is that the IDC can address complex threats to U.S. Army security that must be collaboratively and simultaneously dealt with by several agencies and organizations. This allows the IDC to accurately plan a course of action against asymmetric and asynchronous threats. Leveraging the IDC's advanced technologies to conduct AS&W is transforming the Army's CND capability from a reactive to a proactive posture.

The objective of layering IA tools and technologies throughout the Army portion of the DISN in accordance with Defense in Depth policies is well under way, and reengineering the security of several critical, highly vulnerable legacy systems, such as Domain Name Service (DNS) servers, has been completed. The perimeter-, network-, enclave-, and host-level state-of-the-art security technologies that the Army has integrated into the architectures of the Digitized Division/Corps and the Interim Brigade Combat Team are vital to protecting the Army's substantial investments over the past several years in digitizing the tactical force. Finally, the Army is most enthusiastic about its leadership role in exploring emerging technologies, as exemplified by being designated the DoD Executive Agent chartered to lead, consolidate, and coordinate all biometrics IA activities for the Department. Together, these accomplishments in FY 2000 have proven to be the most significant expansion in the scope and depth of Army IA and CND programs and initiatives since the

Deputy Secretary of Defense issued IA and Cyber Intrusion Detection Action Plan requirements in February 1998.

NAVY-MARINE CORPS

As mandated by the Clinger-Cohen Act, the Department of the Navy’s Chief Information Officer (DoN CIO) is responsible for information assurance within the DoN. To this end, the DoN CIO has implemented policy and continued to take aggressive strides in information assurance throughout FY 2000. To minimize risk to mission-critical and mission support systems throughout the Department, the DoN CIO has focused its efforts on the continuing development of DiD strategies and tools. This section presents an overview of the DoN’s DiD progress and will outline specific DoN IA initiatives. It is followed by Service-specific updates from the Navy and Marine Corps.

CH-46’s ferry supplies from the flight deck of a supply ship to a nuclear aircraft carrier while underway.

For the risk management of sensitive data, DiD information systems depend on multiple layers of protection. Generally, the amount of protection provided should be increased as the sensitivity of the information increases, as the threat increases, and as the operational environment changes. At the outermost layer—or boundary layer—are defensive measures used to limit access to internal net-works. Especially important at connections to the unclassified Internet, these include routers, firewalls, and guards. The DoN also uses intrusion detection systems (IDSs) to identify and prevent unauthorized use, misuse, and abuse of computer systems by both internal network users and external attackers in "near real time." At the enclave layer, DoN Components use antivirus protection software installed on all IT systems to block known malicious code, and the Department is implementing a centrally managed enterprise system that will provide oversight of security applications and update them.

Besides the physical, logical, and technical protections described above, the DoN DiD strategy incorporates proper planning and training. The DoN CIO is implementing a policy that will require comprehensive contingency/continuity-of-operations planning for all DoN mission-critical systems. These plans will provide for rapid emergency response, backup operations, and postdisaster recovery that will ensure that essential functions continue if information technology support is interrupted. Also, DoN CIO will begin requiring all members of the Department to undergo annual user training, with a concentration on Internet security risks and practices. The Department will continue to test the effectiveness of these IA initiatives through regular vulnerability assessments, online surveys, and red teaming.

Making Use of IA Technologies

DoD PKI gives digital identification, signature, and encryption capabilities to a broad range of applications at various levels of assurance. DoN Components continue to aggressively implement the DoD PKI, and the DoN CIO has helped shape the future of the DoD PKI through regular participation in all three PKI Working Groups and the CIO Executive Council. To date, the DoN PKI Registration Authorities have issued approximately 6,300 digital certificates to Navy and Marine Corps personnel and servers. In addition, the DoN CIO hosts a PKI Implementation Conference for all DoN Echelon II Commanders to facilitate their adoption of this technology. DoN users will access DoD PKI services primarily through the Navy/Marine Corps Intranet.

Another example of how the DON is putting IA into practice is the Navy/Marine Corps Intranet (NMCI). The NMCI will positively contribute to enhanced IA throughout the DON in several ways. By providing common COTS-based products and services throughout the Department, current impediments to information sharing and availability will be removed, creating a uniform global network while reducing costs. This enterprise-wide uniformity will facilitate the use of common security tools such as firewalls, provide enhanced network monitoring/intrusion detection, and facilitate trend analysis when it is implemented. Finally, NMCI will provide DON access to the DoD PKI via the new Common Access Card (CAC) and/or other smart card tokens under study by the DON Smart Card Office for use prior to full CAC implementation.

Smart card technology provides the means for identification, authentication, physical and logical access, and electronic transactions throughout DoN, DoD, and the Federal Government. The DoN will use the smart card as its PKI hardware token to authenticate individual access (i.e., verifying an individual's cyberidentity to networks and DoD websites). Once authenticated using their smart card-based PKI credentials, DoN personnel will be able to access information and conduct a multitude of business processes online—securely. Smart cards provide a key technology for implementing and achieving the DoN IA vision. Together with PKI, smart cards will revolutionize the way the Department conducts its business practices and processes. The DoN CIO chairs the DoD Smart Card Senior Coordinating Group and is currently piloting the use of PKI and smart cards for digital signatures, encryption, network access control, and access control to DoN CIO and other DoD secure websites.

The DoN CIO has also been instrumental in the development of specifications and implementation strategies/plans for the DoD CAC, the PKI-enabled smart card to be issued to all uniformed and civilian personnel in DoD. Because of the DoN CIO's expertise in smart card technology, DoD selected that office to prepare a special report to Congress addressing the "Consideration of Smart Cards as the DoD PKI Authentication Device Carrier," submitted in response to a requirement of the FY 2000 Defense Authorization Act.

The DoN CIO recognizes the need for a strong, comprehensive information assurance policy. To that end, it has spent considerable effort updating the Departmentwide guidance for information assurance in a policy instruction scheduled for release in early FY 2001. This policy formalizes the IA concepts listed above and clearly assigns IA roles and responsibilities to major Components of the DoN and to the entire Department in general.

A guided missile frigate makes a turn to port while underway.

In addition to DoD efforts, the DoN CIO participates in the Federal CIO Council and various security-related Federal committees. Through a strategic partnership with BITS (Technology Group for the Financial Services Roundtable), the DoN CIO has participated in several forums on fraud, smart cards, and common criteria that help to further advances in e-commerce and to accelerate initiatives enhancing interoperability between the public and private sectors.

The following two sections present specific Navy and Marine Corps information assurance policies, initiatives, and accomplishments for FY 2000:

Navy IA Efforts

In response to information management/information technology needs, the Navy is changing its organizational structure. The goal is to achieve the timeliest response required for the warfighting needs of rapid adaptation to threats and vulnerabilities. The most challenging areas of information assurance are policy, personnel recruitment, training and retention, availability of technological solutions, large-scale integration, and detailed implementation. All are key parts of a strong DiD infrastructure. The Navy IA program is making great strides in meeting the requirements for technical security protection across the Service. In spite of the progress already made, rapidly evolving technology still calls for vast improvements in IA and will continue to be a major challenge.

The critical infrastructure includes cyber- and physical-based systems essential to the minimum operations of the government and the economy. The Department of Defense must take all necessary measures to eliminate swiftly any significant vulnerabilities to both cyber- and physical attacks on our critical infrastructures, especially our cybersystems. In support of this effort, the Navy has been actively engaged in the Critical Infrastructure Planning Council and working at developing an implementation plan that will support the Department of Defense Critical Infrastructure Protection Plan and Presidential Decision Directive 63. Keeping pace with technology security concerns requires policy derivation and promulgation. Knowledge of existing policies, technical expertise, and real-time operational feedback are major factors for success in this area. On 9 November 1999, the Navy Information Assurance Program Instruction was updated to accommodate the growing need for organizational structure and to create technical security publications more readily adaptable to technical changes. The Navy IA program established specific organizations with specific and nonredundant mission responsibilities for maintaining policy and publications. The program also sought to centralize a technical authority with the necessary understanding of the total security solution and the ability to provide near real-time operational feedback.

The Combat Direction Center (CDC) on board the USS America is the nerve center that gathers specific information.

Policies are being developed very rapidly across the Department of Defense. Navywide web pages adhere to all requirements of the IA community. The Navy IA web page policy provides guidance to publishers of information such as Program Managers. Guidance includes web content security regulations and provides systems administrators with specific technical implementation policy, measures, and tools.

Because of the sensitive nature of these policies, a Public Key authentication-based web server is currently online to ensure that access to this information is limited to authorized recipients. It is necessary, however, to maintain both PKI and non-PKI servers to meet all Navy customer information requirements during the DoD PKI transition.

In accordance with DoD Policy Instruction, the Navy promulgated certification and accreditation (C&A) implementation procedures for separate audiences of PMs and Navy site Commanding Officers (COs) and for the partnership arrangements between PMs and site COs for proper system integration. The procedures, appearing both achievable and executable, have been well received by Navy components to date. A Navywide Information Operations Condition (INFOCON) exercise in late November provided substantive feedback to the operational feasibility of DoD-level policy on INFOCONs. The Navy will continue to work actively at determining the correct balance.

In addition, the Navy is actively pursuing the fielding and development of the Electronic Key Management System (EKMS). Approximately 80 percent of the Navy's legacy, paper-based key and communications security (COMSEC) device management accounts have been transitioned to the electronic form of distribution and management. Of the four tiers that EKMS comprises, the Navy is the lead service for the development of the Common Tier One (CT1), which joins all the Military Services' COMSEC and key management infrastructures into a Joint Service managed environment. The EKMS CT1 is now being integrated into the field at Kelly Air Force Base, San Antonio, Texas; Fort Huachuca, Arizona; and Mannheim, Germany.

While assessing the large-scale Navy needs for PKE, the Navy is still considering the operational unit requirements in the field. The Navy shares with other DoD and Federal Agencies the knowledge gained and lessons learned through assessments and pilot projects. More specifically, the Navy has been focusing PKE attention on evaluating COTS technology responsive to Navy needs and presenting ease of integration into Navy systems.

To support detect-and-respond capabilities, the Navy has increased staffing, thus enhancing support for analysis; increased intrusion detection systems monitoring; and Information Assistance Vulnerability Alerts releasing, tracking, and reporting. In response to higher-authority requests, the Navy is also staffing policy for directed vulnerability surveys.

Seriously working at recruiting and retaining personnel, the Navy has established and promulgated criteria for qualifying systems administrators at all levels mandated by the DoD and established formal training to meet those requirements. Formal training is also offered for the critical position of Information Systems Security Manager, with CND practices and procedures an integral part of this instruction. Commander, Navy Education and Training (CNET) has made maximum use of mobile training teams and local training authorities.

The National Security Telecommunications and Information Systems Security Committee has designated the Naval Postgraduate School (NPS) Center for INFOSEC Studies and Research (CISR) as an Information Assurance Center of Excellence.

In terms of training and education, the Navy needs to meet not only today's growing requirements but also those of the future. In support of this goal, the Navy continues to establish educational infrastructure and to develop and implement a training strategy that includes the following major accomplishments:

- Increased the number of graduates in Communications, Information System, and Networks (CISN) courses
- Established an annual review/update of courses to reflect new technology and application methodologies
- Identified career paths for Navy professionals working in the areas of computer network administration, security, and telecommunications management
- Made available to the Enlisted Community service reenlistment bonus incentives of up to $45,000
- Officially designated more than 20,000 military personnel as information systems technicians and information operations positions

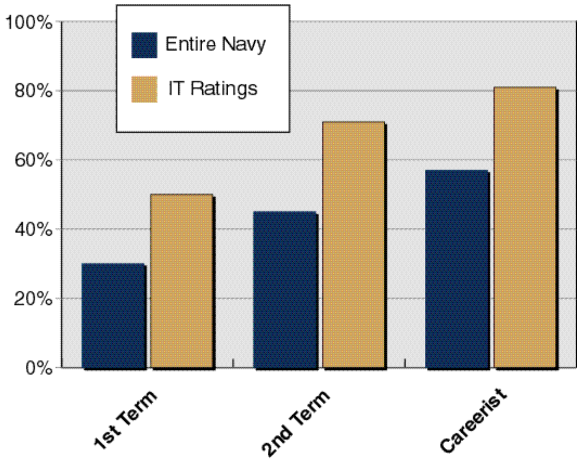


Figure 16. FY00 Retention (IT Rating vs. Navy)

As a result of these initiatives, overall retention across this career path continues to increase.

To address the Defense in Depth concept of defending the boundary layer, the Navy initiated the development of a new, modular, and programmable cryptographic system. The objective is to modernize legacy Navy cryptographic equipment with a system that can support multiple algorithms. Meanwhile, the Navy continued to test for security strengths and weaknesses in COTS firewall, intrusion detection system, and virtual private network products for application to Navy networks. It

The F/A-18 Hornet has proven its capabilities as an all-weather fighter and attack aircraft.

has also begun the transition to developing processes for streamlining the National Information Assurance Partnership® common criteria-evaluated product purchases. The Navy is currently focusing efforts on Network Operations Center (NOC) requirements in providing an integrated package containing security engineering components and integration of firewalls, virtual private networks (VPNs), and intrusion detection complements.

The Navy is fully engaged in fielding secure systems that ease operations across classification levels by providing releasability without compromising security. Efforts continue to field multilevel network and combined wide area network solutions to allow and improve interoperability with foreign navies in every theater around the world for both exercise support and real-world operations. Systems have evolved from man-in-the-loop, text-only e-mail services to the solution set now under evaluation. These include a shared Common Operational Picture, Distributed Collaborative Planning, and automated e-mail with attachments.

The Navy initiated the design of a secure voice gateway (SV21) to interface shipboard-secure voice equipment to a wide range of internal platform networks and connecting systems. The Navy is also developing technology to enable secure voice-over commercial IP networks through a Small Business Innovative Research (SBIR) project that is now in its Phase II. The Navy is currently researching the security of COTS workstations with a plug-in hardware module through two SBIR Phase I efforts. A third SBIR Phase I project focuses on fleet Information Warfare (IW) officers to manage IA resources dynamically through IA battle space visualization technology.

Navy IA is shifting its emphasis from the protection of individual systems to the dynamic management of IA resources at the platform or command level. The protection of the interconnecting networks is following the same trend. Because the information systems themselves consist mostly of relatively unprotected and untrusted COTS products, IA R&D necessarily focuses on the high-assurance components, infrastructure, and system engineering tools required to securely "glue" information systems together. The Navy's objective is to provide a secure infrastructure that allows combatants (i.e., ships, planes, and submarines) to successfully manage IA resources and counterevolving IW attacks.

Marine Corps IA Efforts

During FY 2000, the Marine Corps IA program attained a number of significant accomplishments. Collectively, these accomplishments greatly improved the level of protection provided to Marine Corps-owned and -managed information and information systems. The Marine Corps fully supports a Defense in Depth approach to information assurance. FY 2000 IA activities improved Marine Corps capabilities at every layer of the architecture.

The Marine Corps instituted boundary layer information assurance through the implementation of a decentralized IDS architecture. This IDS architecture reports to a centralized IDS monitoring center and is known as the Marine Corps Intrusion Detection and Analysis Section (MIDAS). MIDAS is a subelement of the Marine Corps Information Technology and Network Operations Center (MITNOC). It is colocated with the Marine Forces Computer Network Defense (MARFOR-CND), allowing rapid coordination and implementation of required actions during network intrusions or CND events. The Marines also fielded and implemented equipment to support VPNs within the Marine Corps. These VPNs target applications that cannot be easily made to comply with established firewall policies are used for the secure remote management of firewalls and network routers from the MITNOC. The Marine Corps' published VPN and firewall policies support this effort by clearly defining areas of operations.

At the enclave layer, the Marine Corps fielded and implemented a number of Deployable Security Interdiction Devices (DSIDs) to support Marine Corps or Joint Service tactical user requirements. Deployed DSIDs and MITNOC teams supported real-world operations in East Timor and a number of exercises involving the 2nd Marine Expeditionary Force, Marine Forces Pacific, and the 7th, 8th, and 9th Communications Battalions. As part of an enterprisewide program to reduce the impact of malicious code, the Marine Corps has also successfully implemented a highly effective server-based antivirus software that is centrally managed to ensure standard configuration and rapid update dissemination.

The Marines had to modify their PKI program milestones because of the alignment of the PKI and access card programs. The upgrade of the Defense Eligibility and Enrollment Reporting System/Real-Time Automated Personnel Identification System (DEERS/RAPIDS) infrastructure to support PKI registration will begin in January 2001. The contract for conventional PKI registration and director y services support for the Marine Corps was awarded in August 2000. Fielding of conventional local Registration Authority workstations and directory servers will begin during November 2000. Approximately 1,500 Class 3 PKI identity and e-mail certificates have been issued through the USMC Registration Authority to support e-mail and web server access pilots. Approximately 63 private USMC web servers have registered for server certificates.

In response to concerns regarding the necessity to safeguard information systems, the Marine Corps has developed a Corpswide awareness training program that includes Headquarters C4 coordinated base visits that will ensure the continuity of information provided to Marines. Although the Marine Corps has been effective in safeguarding information, additional measures will be implemented.

The Marine Corps is integrating its Critical Infrastructure Protection (CIP) and its Continuity of Operations Planning (COOP) activities. The complementary objectives are to minimize disruptions in operations and to immediately resume essential functions in the event of an emergency. Currently, the Marine Corps is identifying and prioritizing assets that enable Marine Air-Ground Task Force (MAGTF) mobilization, deployment, sustainment, and mission execution in support of Commander-in-Chief operations plans. In response to the threat of malicious intrusions, the Marine Corps developed a Continuity of Operations plan for all echelons of the Marine Corps Enterprise Network. The plan provides guidance on how to continue operations of automated processes in the event of a malicious intrusion or disruption.

Navy

AIR FORCE

Current Air Force (AF) warfighting capabilities and those envisioned for the year 2020 require a robust IA capability. Key to AF IA capability is a DiD strategy that integrates operations, people, and technology for multilayered, multidimensional protection. IA capabilities must be built in through a well-documented command, control, communications, computers, and intelligence (C4I) support plan as new C4I systems are developed, rather than added on after system development. At the same time, personnel must be trained and educated to embrace the concept that in our integrated communications environment, an IA risk to one or through one is a risk to all.

IA Strategy and Planning

The IA Strategic Plan developed by the AF revised and expanded its IA strategy. The plan integrates the policy, guidance, capabilities, and program oversight to empower twenty-first century aerospace operations and to integrate IA into an enterprisewide, networkcentric concept. The current AF strategy gives to users, operators, developers, maintainers, and program managers of communications and information systems the security, processes, training, and tools required to protect information and information systems, thus ensuring availability, access, integrity, authentication, confidentiality, and nonrepudiation of information with maximum efficiency and effectiveness. The AF is expanding this strategy to emphasize integrated network operations and information protection, automated and dynamic detection and response, consolidated situational awareness and decision support, IA throughout the life cycle of all programs, and IA in deployed and classified environments. A newly developed senior officer steering group, as well as new revisions to Air Force policy, have been put in place to ensure that the evolving strategy succeeds.

The Air Staff conducted the first-ever Information Operations General Officer Steering Group. This unprecedented event served as an excellent forum for greater partnering of all the Air Force Information Operations (IO) Components in accordance with Air Force Doctrine Document (AFDD) 2-5, Information Operations. An important outcome of this forum was an agreement to revise AFDD 2-5 and to introduce the concept of Information Services—including IA—as an integral part of IO.

The AF also established a cross-functional IA Panel (IAP), intended to provide to the Air Force Chief Information Officer (AF-CIO) a senior-level brain trust to develop and coordinate AF IA positions. Representatives from across Research and Development, Acquisition, Policy, and Operations communities convene on a quarterly basis to review AF IA strategy, policy, architectures, technology, programs, and associated funding requirements. The IAP's intent is to provide a clear and consistent IA policy, mitigate duplication of efforts, focus organizational responsibilities, and help ensure that the AF has the resources to implement its IA strategy.

As its understanding of IA, technology applications, and mission needs matures, the AF will remain committed to helping policy and guidance evolve. Integral to this effort is optimizing the balance between security and warfighter requirements. This approach was applied in the development of new AF policy and guidance. First, the ad hoc deployment of personal digital assistants (PDAs) warranted that AF personnel be notified of the potential security vulnerabilities associated with this equipment, as well as with policy governing the use of these devices within the AF enterprise. The published AF policy was provided to ASD(C3I) to assist in its efforts to develop DoD policy addressing digital devices. Second, increased requirements for foreign national access to the Not Classified but Sensitive Internet Protocol Router Network (NIPRNET) prompted the publication of additional guidance that identifies the process to follow according to the different foreign national (FN) support categories. For example, FNs who are part of the Defense Personnel Exchange Program (DPEP) are subject to a less rigorous process than FNs hired as contractors. Finally, the AF is diligently working to establish, in concert with the Joint Staff, a mobile code policy. Recently, the AF sponsored a proposed mobile code operational test to determine the impact on missions if the policy is implemented. The test results were given to the Joint Staff and should help to shape this directive.

> *“Our recent Year 2000 experience confirmed that Aerospace Forces depend on information technology to perform their day-to-day mission. In the future, our dependency on information and on our critical information systems will only increase as we employ our expeditionary forces. The need to protect and ensure voice, video, and data must remain a priority if we are to continue to provide timely, trusted, and reliable information to the warfighter.“*
>
> *- Lt. Gen. (Ret.) William J. Donahue*
> *Director, Communications and Information,*
> *The State of Information Assurance in*
> *the United States Air Force*

To improve new system supportability and security, the AF-CIO released Air Force policy requiring development of Command, Control, Communications, Computers, and Intelligence Support Plans (C4ISPs). The policy directs developers of new systems to identify and resolve C4I issues (e.g., compatibility with existing C4I infrastructure, security, and sufficient life-cycle logistics to include personnel and resources) before systems are fielded. An integral C4ISP process is network risk assessment testing, which identifies security problems and proposes remedial actions to the Program Manager (PM). Systems deemed "networthy" (those that pose little or no risk to the AF enterprise network) are granted a Certificate of Networthiness (CON) either by the AF-CIO for AF or DoD-wide systems or by the Major Command (MAJCOM) CIO for MAJCOM unique systems. The C4ISP process is presently at work: several security problems have been identified and referred to PMs for resolution.

As part of the AF Modernization and Planning Program, the AF published an Information Warfare Mission Area Plan (IW MAP) for FY 2000. The IW MAP creates a framework for military planners, operators, and developers for a better understanding of the IW mission area and outlines a notional long-term investment strategy. As reflected in the AF's top IW needs, IA and CND are paramount in the modernization planning process. The AF has also initiated the FY 2002 IW MAP, which will include a separate IA Annex and will expand the IA scope to include integrated network and security operations infrastructure and activities.

During the past year, the Air Force developed a concept to move from stand-alone information systems supporting individual functional communities to "netcentric" operations that use web-enabled applications supporting multiple users. Netcentric operations are accomplished when warfighters can trust and depend upon the information carried by the communications and computing transport layer. Application of IA to the netcentric Air Force will guarantee the confidentiality, integrity, availability, authentication, and nonrepudiation of information anywhere, anytime, and on any platform across the Air Force Information Enterprise (AFIE). The Air Force is in the process of installing network and security operations at regional enclaves to leverage scarce resources currently used to defend assets at more than 100 installations. This regionalization effort will enhance security by focusing Air Force expertise on defensive countermeasures at critical junctures, protecting the gateway to a trusted Air Force intranet.

The Air Force implemented the Status of Resources and Training Systems (SORTS) criteria identified in Air Force Instruction (AFI) 10-201. The stated AF objective is to operationally achieve C-2 at base Network Control Centers (NCCs), MAJCOM Network Operations and Security Centers (NOSCs), and the Air Force Network Operations and Security Center (AFNOSC) not later than the end of this year. When the Air Force began this initiative, it initially assigned itself a readiness level at C-5 for all units. By midsummer 2000, the Air Force was well on the way to achieving its objective, with a majority of units better than C-5. SORTS status is briefed to the Secretary of the Air Force on a quarterly basis.

Network Management and Security Architecture

The Air Force has continued to build on the capabilities of its three-tiered network management and security architecture. At the global level, the AFNOC and the Air Force Computer Emergency Response Team (AFCERT) responded to network-based threats such as the "ILOVEYOU" computer virus to minimize impact to AF network operations. The AFCERT continued to lead computer network defense efforts while overseeing network anomaly monitoring and analysis by the Air Force's intrusion detection system (IDS), the Automated Security Incident Measurement System (ASIMS). To keep up with the evolving threat, ASIMS attack signatures will continue to be updated with the latest hacking techniques to ensure early warning of attempted penetrations into AF networks.

> *"Because these information capabilities are so valuable as weapons, they are also lucrative targets that are under threat of harm in all national security situations from peacetime through full-scale war."*
>
> *- Lt. Gen. John Woodward*
> *Director for C4 Systems, The Joint Staff*
> *IA Through Defense in Depth, February 2000*

Network Operations and Security Centers (NOSCs) at each of the MAJCOMs played an ever-increasing role in AF IA processes. Overseeing network operations in each of their respective areas of responsibility (AORs), NOSCs ensured network availability, monitored network operations, and responded to system intrusions/viruses. The NOSCs played a significant role in combating the "ILOVEYOU" virus and related viruses that hit Air Force networks in spring 2000. Their ability to react to the virus attacks and to direct NCC actions was significantly better than responses to the "Melissa" virus attacks in 1999. Demonstrating even more improvement, NOSCs implemented enhanced dissemination, tracking, and reporting oversight of AFCERT's Advisory Compliance Messages, thereby helping to reduce the number of network intrusions from 1999.

At the unit level, base Network Control Centers (NCCs) acted as the focal point for many IA issues. Working with the wing IA office, NCCs provided network operations and security functions on the network front lines. NCCs were responsible for assuring literally all network transactions taking place on Air Force installations. At the same time, they positioned our networks for new threats by responding to more than 10 network/system vulnerability advisories distributed by AFCERT.

AF IA organizations continued to play a key role in CND. The Commander, Air Force Forces (COMAFFOR) JTF-CND worked with MAJCOM NOSCs to further address the evolving role of the JTF-CND. The Air Force developed procedures to accomplish JTF-CND tasks and report to appropriate organizations.

Managing IA

Continuing to focus on AF IA issues, the Air Force Audit Agency (AFAA) completed two IA-related audits: "Implementing Controls over Known Vulnerabilities" and "Certification and Accreditation." In addition, AFAA has completed the fieldwork for two more IA-related audits: "Air Force Research Laboratory UNIX-Based Computer Systems" and "Web Page Management." Future audits within the AF IA realm include "Database Security Controls," "Supercomputer Shared Resources," "Sanitizing of Personal Computers Prior to Disposal," and "The Secret Internet Protocol Router Network." The AF also participated in two General Accounting Office audits related to IA: "Incident Response Capabilities" and "DoD Information Assurance Program." Finally, to follow SII 99-04, the Air Force also instituted an Inspector General (IG) Special Interest Item (SII) for IA: SII 00-02, IA Program. For the first 60 days of SII 00-02, units were directed to conduct a self-inspection. The remaining period, 1 May 2000 to 31 October 2000, will serve as a formal inspection period. The SII provides feedback to AF leadership on the effectiveness of IA training programs; wing/base leadership involvement; and adherence to AF IA directives, policies, and procedures.

> *"'Total Force' awareness among active duty, guard, reserve, civilian, and contractor personnel is vital to maintaining a mission-ready posture. Significant increases in all aspects of user training demonstrate the AF's concerted effort to equip our personnel with the requisite IA familiarity and awareness."*
>
> *- Lt. Gen. (Ret.) William J. Donahue*
> *Director, Communications and Information*
> *The State of Information Assurance in the United States Air Force*

The AFNOC has been making progress (1) in determining the mission areas/processes/products that are important to improve and for which to develop a baseline and (2) in tracking this information to ensure that the Air Force's IT investments are, in fact, bringing improvements. The Air Force was the first to implement Enterprise Operations Metrics. Although still in the early stages of implementation and focusing on product and quality of service, these metrics have helped determine ways to improve security awareness, training needs, and operational needs to ensure a healthy network. The metrics address Air Force-wide premise router availability, circuit availability, intrusion detection, and Domain Name System (DNS) server availability. Other metrics address infrastructure network operations. The Air Force is moving toward metrics and tools that provide a more complete operational picture of the network; it should meet this goal by the end of this year. The Air Force is working with the other Services and Agencies to develop a standard set of metrics for the DoD that clearly define acceptable levels of service for all users.

The AF, in accordance with Air Force Instruction 33-205, "Air Force Information Protection Metrics and Assessment Program," collected metrics to produce "The State of Information Assurance in the US AF 1999" (published March 2000). This report was provided to the AF Deputy Chief of Staff, Air and Space Operations (AF/XO) in order to develop the first-ever Defensive Counterinformation (DCI) Annual Assessment. In accordance with AFDD 2-5, "Information Operations," six core disciplines form DCI: Information Assurance, Counterintelligence, Operational Security (OPSEC), Counterpsychological Operations, Electronic Protection, and Counterdeception. The AF is also participating in the DIAP effort to define AF IA Readiness metrics. This process will be leveraged to refine the IA assessment program.

IA Training

The AF is aggressively working to meet the ASD(C3I) mandate that all unclassified users and systems administrators be trained and certified by 31 December 2000; therefore, the AF developed and deployed a comprehensive Information Systems (IS) User's Course. The IS User's Course will be adopted to fulfill IA training through the Security Awareness Training and Evaluation (SATE) program. Recognizing the exponential growth of web-based technology, the AF is developing a computer-based training (CBT) program for personnel responsible for web- and pagemaster duties. Increased IA awareness among web professionals should bolster the AF network security posture.

The Air Force developed a Professional Certification Guide (PCG) for 11 possible crew positions for all tiers of the operational hierarchy. Since CBT became available in April 2000, 32 percent of AFNOC personnel have completed a portion of the core training requirements and 23 percent have completed additional AFNOC formal training requirements. The AFNOC has made great strides in contributing to managing, protecting, and assuring aerospace information capabilities. The Air Force continues to strive to ensure that information resources are supporting aerospace operations across the entire spectrum of operations in all environments.

Information Assurance

Operationalize

- **R**eadiness
- **I**nspect/Evaluate
- **G**raduated Response
- **O**perational Reporting
- **R**ules of Engagement

Professionalize

- Organize (Tiered Structure)
- Train (Certification)
- Equip (Standardization)

Figure 17

It is critical that the Air Force have in-house technically savvy and situationally aware analysts who can perform enterprise-level duties. Air Force information professionals as a whole and AFNOC personnel in particular must effectively perform strategic, Air Force-wide correlation of network events in order to manage the operation of the network in a structured, disciplined manner. To match more closely weapons system operators and processes of maintainers, the Air Force adopted "RIGOR" to change the way that it trains, organizes, and equips its network professionals. The information requirements of the Air Expeditionary Force Commander and other Air Force decision makers can only be satisfied by rigorously engineered and interoperable protected networks, staffed by certified communications professionals. In order to "train as we fight," it is important to standardize Air Force network operations and management by aligning with joint network operations and management efforts.

Qualified Air Force people are key to our IA success. The Air Force is making sure that its network operators have initial qualification, mission qualification, and continual training so that the people who operate and maintain networks are licensed and certified. Just as aircraft maintainers must be certified before working on an aircraft, network operators must be certified before working on a network. Users earn their "license" by demonstrating the ability to competently use network protection resources. By licensing users and certifying network operators, the Air Force is ensuring that all personnel responsible for protecting DoD information have demonstrated the competency needed to perform their tasks. To this end, the Air Force has implemented a Mission-Essential Task List (METL) process and is strictly enforcing mission qualification to ensure that only mission-ready people deploy, thus improving support for combat operations.

Finally, the AF is embarking on a yearlong IA campaign plan, which will include a monthly theme focusing on IA topics relevant to all airmen. The theme will impart the concept that IA is the responsibility of all Service members. IA topics range from the threat to web security to network professional responsibilities.

This year, the Air Force implemented the ASD(C3I) policy (dated 22 August 1999) to identify and terminate all connections to Internet Service Providers (ISPs). The ISP Termination Policy has helped the Air Force make great strides in protecting its networks against intrusion and malicious activity. Several Air Force connections to ISPs were terminated. Eighteen ISP waiver requests were submitted for special Air Force mission requirements. The majority of Air Force ISP connections were implemented for special mission requirements (information operations, electronic business, and electronic commerce connectivity) or to provide interim compensation for existing shortcomings in DoD’s Internet gateways until they are upgraded.

Intrusion Management

The Air Force continues its efforts to identify suspicious connections to networks. The identification and the recording of these connections are performed by the Automated Security Incident Measurement System (ASIMS). Suspicious connections that fall outside the norm (multiple connections to an Internet Protocol (IP) within a specified time frame, connections between systems that do not normally connect, etc.) are identified, and actions are taken to eliminate those connections by closing back doors and improving overall mission security and network reliability.

The Air Force's "Data Point" program is used to identify the number of intrusions during the month (number of suspected intrusions/number of suspicious connections). Overall, the Air Force has seen a decrease in network intrusion for the year, an indication that its defenses are improving. The use of security checklists in the Air Force Network Operations Center (AFNOC) supports this trend.

Front view of an E-3 Sentry Airborne Warning and Control System in-flight.

As part of the Network Management System/Base Information Protection (NMS/BIP) program, the Air Force purchased and fielded a commercial host-based intrusion tool used to detect unauthorized activity on network devices.

Making Use of IA Technology

The DoD recently established the Biometrics Management Office (BMO) and appointed the Army as its Executive Agent. The Air Force is a full partner in this organization. The Air Force is in the process of sending a full-time representative to the BMO. Projected activities during FY 2001 are (1) develop AF Biometrics Strategic Plan, (2) determine AF requirements, (3) research any legal hurdles to implementing biometrics in AF, and (4) initiate biometrics pilot programs.

For several years, firewalls have been installed in AF NCCs worldwide. To enhance Defense in Depth capabilities, the Air Force installed additional firewalls and upgraded existing firewalls to new software versions at 108 locations. This project includes additional firewall training for local network operations personnel, as well as the fielding of improved network management tools. The project will continue in calendar year 2000 and is scheduled for completion by early 2001, eventually enhancing firewall operations at all Air Force installations.

Another IA improvement came from implementing Virtual Private Networks (VPNs) to protect sensitive information (e.g., financial and medical) within the Air Force intranet. These VPNs secure the AFNOC network router management capability, as well as other sensitive data on the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET).

By using the DoD PKI certificates to digitally sign e-mail and electronic documents and forms, the Air Force is increasing the data integrity and nonrepudiation of the information transferred across Air Force and DoD networks. The digitally signed document indicates to the recipient that the document has not been modified while in transit. In the case of contractual documents, the digital signature on a document provides proof of authorization without a "wet" signature.

Since early 1999, the Air Force has acted as a key partner of the DoD PKI program. The Air Force is moving forward to establish an infrastructure that will allow it to reap PKI benefits. The Air Force is working to satisfy DoD milestones through its PKI System Program Office (SPO). To comply with directed milestones, the SPO is implementing PKI directory services, certificate management processes, certificate issuance infrastructure, and deployment of certificates. The SPO is executing procurement and operations focused on supporting the Air Force PKI Implementation Plan. Currently, the Air Force PKI program is issuing PKI certificates to individuals involved in pilot programs that use DoD public key technology to secure information exchange and business process applications. The focus of the pilot participants is to secure patient data for the ACC Surgeon General's office, secure source selection data for the Strategic Nuclear Deterrent Command and Control SPO, encrypt and digitally sign e-mail for AFOTEC participants, and provide digital signatures for the Defense Travel Service application. The AF PKI SPO is also involved in the education and training of Registration Authority personnel who implement all user registration for certificates and certificate management activities. This year, it has trained more than 30 Registration Authority personnel and has also established a Test and Integration Cell, providing technical support to 11 AF application developers that are enabling their applications to use public key certificates for digital signature and encryption services.

The Air Force PKI program is working on a parallel effort with the DoD Access Card Office to integrate the common access card (CAC) as the primary token for DoD PKI certificates. This will greatly enhance the security and portability of DoD PKI certificates. In FY 2000, the Air Force issued more than 6,000 certificates and is aiming at a total of 700,000 certificates by FY 2003. The Air Force will continue to enable Air Force applications to take advantage of the security and IA enhancements that PKI provides. The Air Force Portal, enabled with PKI technology, is the next step forward in providing secure applications and content throughout a netcentric Air Force.

Agencies

BALLISTIC MISSILE DEFENSE ORGANIZATION

The Ballistic Missile Defense Organization (BMDO) is responsible for managing, directing, and executing the Ballistic Missile Defense Program. The BMDO's program objective is to develop and deploy increasingly capable Theater Missile Defenses (TMDs) to meet the existing missile threat to deployed U.S. and Allied forces. As a hedge against the emergence of long-range ballistic missile threats, the BMDO also seeks to develop options to deploy a National Missile Defense (NMD) for the United States. Lastly, BMDO is continuing the research on more advanced ballistic missile defense technologies to keep pace with the threat and to improve the performance of theater and NMD systems.

BMDO has taken an active role in the development of IA programs throughout the Department of Defense. One in particular is the Secondary Heuristic Analysis for Defensive Online Warfare (SHADOW) program. With BMDO support, this award-winning, Joint Service intrusion detection system (Government Technology Leadership Award, December 1998) developed new features such as host-based and network-based analysis functions and a new capability that performs predictive analysis. Other new features include a Transmission Control Protocol (TCP) analysis tool to identify network traffic anomalies in packets/sessions, the addition of a database tool that integrates with Nmap (a utility for port-scanning large networks) for vulnerability profiling, and a version that now runs on Microsoft NT platforms. The SHADOW development effort was recently honored with a System Administration Networking & Security (SANS) Institute 2000 security technology leadership award.

In 1998, BMDO implemented one of the first corporate vulnerability assessment programs for administrative networks, based on guidance published within the DoD by the Deputy Secretary of Defense. ASD(C3I) praised this effort as a model for the entire Department. Then and now, the program's significant elements include a thorough, objective component showcased by commercial and proprietary tool sets to determine vulnerabilities, network traffic anomalies, device validation, and web/e-mail content. The second component focuses on conducting a thorough assessment of a site's functional areas by interviewing area representatives with an empirical survey tool. In 1998–1999, BMDO baselined both headquarters and subordinate commands by applying this methodology. This process has matured into cyclical second-level activities of ongoing problem correction and revalidation.

Performing vulnerability assessments in weapons systems and their related areas has provided unique challenges in joint certification and accreditation (C&A) efforts. BMDO is successfully partnering with Services and sister Agencies to complete C&A activities while reducing cycle time and minimizing costs for personnel/financial resources.

In another effort, BMDO is seeking answers to one of the most pressing questions that the Defense Information Assurance Program Office must address, "How much does a pound of IA cost?" BMDO has joined forces with DIAP personnel to create a cost model that can successfully span administrative, mission, and weapon systems so that Program Managers can accurately benchmark and advocate their Information Assurance requirements.

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

The Defense Advanced Research Projects Agency (DARPA) is the central research and development organization for the Department of Defense. It manages and directs selected basic and applied research and development projects for DoD. Its other responsibility is to pursue research and technology with high risk and potential payoff that, if the agency is successful, can dramatically advance traditional military roles and missions.

Information Assurance and Survivability Program Suite

The DARPA Information Assurance and Survivability Program Suite (IA&S) seeks to reduce cybervulnerabilities and to give commanders the insight and control necessary to defend mission-critical information systems. In cooperation with civil authorities, U.S. forces will better maintain information battlespace dominance in protecting not only their own systems but also the U.S. "cyberhomeland," thus reducing adversaries' ability to strike at our national security through our information systems. The IA&S programs are a coordinated, cooperatively managed suite of programs. Working in concert, they help develop advanced mechanisms and systems to assure DoD and Critical Infrastructure systems against cyberattack. IA&S seeks to improve system defense capabilities against sophisticated adversaries. Its focus is on creating design techniques, tactical and strategic operational control techniques, and advanced flexible technology to allow critical information systems functionality. During FY 2000, IA&S met a wide range of technology challenges surrounding the eight programs that make up the suite and that are in various phases of development. The first six are located in the DARPA Information Systems Office (ISO), and the last two in the Information Technology Office (ITO):

- The Information Assurance (IA) program seeks to discover principles such as static and dynamic layering (Defense in Depth) that allow trustworthy systems to emerge from relatively untrustworthy components.
- The Information Assurance Science and Engineering Tools (IASET) program seeks to create a science-based environment for system design and assessment that will yield improved information assurance and eventually allow for faster design and assessment at less cost.
- The Autonomic Information Assurance (AIA) program seeks to create an operational systems control framework that can autonomously detect, and tactically respond to, high-speed and known classes of cyberattack.

- The Cyber Command and Control (CC2) program seeks to create an operational human decision-making framework by creating cybersituation understanding techniques and course-of-action generation and analysis techniques. These provide the ability to orchestrate actuators to carry out an effective information warfare defense even when systems are imperfect and resources limited.
- The Strategic Intrusion Assessment (SIA) program seeks to create correlation and fusion algorithms to improve detection of sophisticated, large-scale distributed attacks and to reduce false-positive rates.
- The Intrusion Tolerant Systems (ITS) program seeks to create ways of allowing systems to support critical functions in the face of successful attack.
- The Fault Tolerant Networks (FTN) program seeks to ensure continued availability and graceful degradation of the network infrastructure in the face of network-level attacks.
- The Dynamic Coalitions (DC) program seeks to enable secure collaboration within dynamically established mission-specific coalitions while minimizing potential threats from increased system exposure or compromised partners.

Late in FY 2000, the ISO programs of IA&S were reorganized and placed in a larger program called the Third-Generation Security (3GS) Program Suite. 3GS focuses more on systems and operational experimentation so that it can address urgent DoD IA needs and proactively move to enhance and protect our tactical and strategic advantages. 3GS began execution on 1 October 2000 in coordination with the FTN and DC programs.

The DARPA IA continued its experimentation efforts to pursue science-based, hypothesis-driven experimentation that focuses on "dark spaces" of IA&S, categorizing the "hard problems" not dealt with by the COTS community or other government programs. It sought to refine the experimentation process to ensure that resources would be well spent and that scientific objectives would govern execution. In doing so, it took advantage of the DARPA IA Laboratory, which comprises more than 70 computers, networking, and Virtual Private Networks (VPNs) for remote collaboration, allowing experimentation in a controlled environment.

The four phases of the DARPA IA program are hypothesis development, technical objective and approach identification, experimentation, and transition. The theory and planned implementation of the last two phases are developed during the hypothesis and technical objective and approach phases. Examples of hypotheses are (1) that trusted systems can be composed of less trusted components and (2) that dynamic defenses improve system assurance. Objectives are formed from such hypotheses. An approach is then devised that leads the scientists to discover new technologies or new uses for existing technologies. In the experimentation phase, DARPA takes a science-based approach, using focused experiments and red teaming to understand user requirements and to enable the technology transition to a useful product. In the transition phase, DARPA seeks to create markets for its technology, transfer its knowledge to those who need it, and partner with important DoD activities to test and field products.

Part of the experimentation phase described above is Scientific Red Teaming. DARPA refined the nontraditional role of the red team as a cooperative partner engaged in experimentation and learning and identified major differences between defender and attacker approaches. In so doing, DARPA was able to categorize adversary behavior focusing on techniques to thwart adversary planning, preparation, and attack execution. DARPA also instituted an offshoot of red teaming known as "whiteboarding." It is an efficient, cost-effective early step in the experimentation process through which attackers and defenders discuss their approaches in a particular scenario. If opposing sides agree on results, then it is likely that actually performing the experiment may not make sense. On the other hand, if opposing sides disagree, an experiment usually takes place.

DARPA has developed a specific and tactical definition for Defense in Depth (DiD) that focuses not only on only successive layers of defense but also on the breadth of defense within each layer. In the cyberarena, "depth" implies multiple defense mechanisms against a particular attack class, while "breadth" addresses multiple attack classes spanning a broad attack space.

"Defense in Breadth" is a key element of Defense in Depth in the cyberarena. Cyberadversaries may possess many attack tools, but they will invariably use the attack with the least risk and expense. This is referred to as the "lowest picket in the fence" phenomenon.

Another focus of DARPA efforts this year was on adversary behavior. It was determined that adversaries spend up to 95 percent of their time preparing for attack and that risk-averse adversaries lower their risk tolerance thresholds as attack time approaches; therefore, the ability to increase adversary uncertainty is a good defense technique. Keeping adversaries guessing during preparation time increases uncertainty and may preclude attack launch altogether. An example of this technique is dynamically switching IP addresses of the enclave to be protected.

Local Computing Enclave and Enclave Boundaries

In defense of the local enclave and its boundaries, DARPA further developed the Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD) as an advanced intrusion detection architecture and sensor system. It’s been proven to perform significantly better than COTS intrusion detection systems (IDSs), and it has been effectively deployed to operational sites for experimentation [such as the Joint Intelligence Center, Pacific (JICPAC) in Hawaii].

The Intruder Detection and Isolation Protocol (IDIP) was refined as an architecture and capability for managing Intrusion Detection and Response. It was initially intended as a way to rapidly prove concepts, but is now beginning to evolve into an integrated system with significant potential. One of its main benefits is its potential for WAN application.

DARPA has been developing dynamic address translation (DYNAT) to work in conjunction with conventional intrusion detection systems. DYNAT is a TCP/IP Spread Spectrum technique for closed communities that is principally based on dynamically switching IP addresses for community members. This dynamic switching spreads a fixed number of IP addresses over a broad address space that requires external correspondents to be synchronized with the address-switching algorithm. The system is then able to isolate attackers and others without the current IP with near-perfect ability.

DARPA has also developed significant "wrappers" technology. Wrappers can provide elements of trusted path and control (for example, between a keyboard and a smart card) and protection against writing to removable media and safe execution environments. DARPA developed operating systems wrappers for Windows NT, Windows 2000, Solaris, and Line. They provide significant capabilities in host protection.

DARPA has expended a great deal of effort in the area of intrusion tolerance, which is based on the premises that network attacks will occur and that some will be successful. These attacks may be coordinated across multiple sites or in a single effort. The operating hypothesis is that attacks can be detected, contained, and tolerated, enabling mission-critical applications to continue to operate correctly.

An intrusion tolerant system is defined as one that can continue to function correctly and provide the intended services to the user in a timely manner in the face of an attack. The emphasis is on maintaining data and program integrity in the face of intrusions and malicious faults and to counter denial-of-service attacks and maintain high system availability. Intrusion tolerance is achieved by developing technologies that exist beneath the layers of traditional defense mechanisms. These technologies are functionally categorized as follows:

- **Execution monitors** – Work includes developing secure mobile code format, execution monitors, protection from malicious hosts, scalable proof-carrying code compilers, and technologies to sandbox active scripts and to monitor COTS binaries.

- **Error detection and tolerance trigger s** – Work includes digital integrity marks, application-based error detection, and redundancy-based detection.
- **Error compensation, response , and recovery mechanisms** – Work is being done in component location elusiveness; fragmentation, redundancy, and scattering; spatial, temporal, and design-diverse architectures with randomness and uncertainty; and quality-of-service trade-offs.

During FY 2000, many useful products have emerged from the intrusion tolerant technology efforts. An effective signature-independent defense to the recent "ILOVEYOU"-type e-mail viruses that use VBScript was developed and deployed. A promising architecture using fragmentation, scattering, and redundancy to tolerate malicious code and denial-of-service attacks was demonstrated in July 2000. In addition, techniques for monitoring the behavior of applications during execution are nearing the demonstration phase, and a scalable compiler for code that carries trust certification proof is nearing prototype. A wrapper technology that prevented the introduction of malicious code by e-mail was demonstrated as an early result of a project working on integrity through mediated interfaces. Also, a technique for "sandboxing," or isolating active scripts while monitoring behavior, was also demonstrated in July 2000. Finally, promising progress was also made in a project working on making legacy code safe by injecting binary agents into the existing program.

Networks and Supporting Infrastructure

DARPA worked on two projects regarding networks and supporting infrastructure: intrusion assessment and cybercommand. These technologies can discern and assess coordinated attacks and enable response at the appropriate levels—autonomic or human command and control—along three distinct, but interrelated, axes of research:

- The first axis seeks correlation between sensor and network performance data and the development of algorithms analyzing sensor information and automated techniques, allowing a tracking of the nature of incidents and event histories.
- The second axis is to improve coordination between anomaly detectors. Creating the ability to share event information allows local detectors to exploit global information and focus local capability by tuning detector sensitivity. This track seeks to develop common languages for exchanging event information and coordinating response.
- The third axis focused on sensor placement characteristics under a concept for layered compositional intrusion detection which can be achieved through pooling the effects of distributed, diverse sensors. The aggregate goal for this approach is to be able to recognize strategic attacks in real time and sustain the flow of relevant information for use by cybercommand and control entities,

while significantly reducing the incidence of false alarms (false positives) and detection failures (false negatives).

In the area of intrusion detection system evaluation, DARPA's Strategic Intrusion Assessment (SIA) program operates the only evaluation of intrusion detection systems (IDSs) that is recognized for using a scientifically valid process. The evaluation program is designed to assist sensor developers in improving the progress of their individual projects, thereby increasing the capability of the sensors. Continued improvements were made in the evaluation design and execution process throughout FY 2000 as the result of outcomes from several workshops and conferences.

DARPA worked on IDS reporting. A working group of developers studying the area of attack report aggregation and correlation developed an Application Program Interface (API) to help specify and communicate the properties of intrusion detector reports needed for effective correlation, along with a rationale. The API was intended to be representative of a more complete detector-reporting API. It was designed to accommodate both signature-based detectors and anomaly detectors. Because of the wide range of detectors envisioned, the number of required elements was limited to the unique identity of the detector and the time of detection. The API is designed to accommodate a number of transport mechanisms, including files (the most likely mechanism for an offline evaluation), and a number of formats, including the XML-based format specified in a draft Request For Comment (RFC) developed by the Internet Engineering Task Force (IETF) Intrusion Detection Working Group. It also uses ANSI C to provide greater portability among intrusion detector platforms.

DARPA also developed technology in the area of fault tolerant networks. Research is being conducted to improve fault tolerance and survivability of networks. Funded in partnership with the National Security Agency (NSA), the Laboratory for Telecommunication Science (LTS), and the Air Force Research Lab - Rome (AFRL), more than 20 new projects are in progress in the following areas:

- Fault Tolerant Survivability
- Denying Denial of Service
- Active Network Response

Military Commanders increasingly need to operate and communicate with coalition partners. DARPA has coordinated efforts with several other government groups, including the U.S. Central Command (CENTCOM) and the Joint Forces Command (JFCOM), to obtain input from operational forces regarding the types of products that they will need in the near term. In support of this requirement, more than 20 new DARPA projects, several of which are cofunded by NSA, are in progress in the following areas:

- Coalition Infrastructure Services
- Policy-Based Security Management
- Secure Group Communications

"Cybercommand" refers to providing insight concerning the state of cybersystems, attacks, and courses of action. In the area of cybercommand functions, DARPA developed an early prototype of a command-and-control tool for the cybercommander and a management tool for visualizing the cybersituation of a given network, assessing courses of action, and responding appropriately. Cyber Command System (CCS) uses an advanced object-oriented database, publish-subscribe technique, and middle manager concept in a flexible hierarchical framework. DARPA developed initial situation analysis techniques to derive strategic attack hypotheses. It also demonstrated a prototype system for dynamic retasking of sensors to acquire missing situation information. Another effort resulted in the development of capabilities for analysis and execution of directly controlled strategic response elements.

DARPA established a mutually beneficial experimentation relationship with USCINCPAC, JICPAC, and DISAPAC, allowing a better understanding of real operational requirements and improved planning for ultimate deployment and life-cycle support. The Agency also initiated planning for significant experiments with PACOM in FY 2001 and laid the foundation for a Partners in Experimentation program beginning in FY 2001. An evaluation edition of eXpert-BSM, an intrusion detection system developed under the SIA program by SRI International, is being made available to the public for free download via the Internet. eXpert-BSM is a component of the SIA program's EMERALD project. eXpert-BSM is a host-based intrusion detection system for the Sun Microsystems Solaris operating system, a computer systems platform widely used in the DoD and industry.

Third Generation Security

Late in FY 2000, the ISO programs of IA&S were recast to the Third-Generation Security (3GS) Program Suite, which has a greater systems and operational experimentation focus. The 3GS Program Suite comprises three technology development programs, an early operational experimentation program, and a systems development program. First-generation security emphasized keeping intruders out through the use of such means as trusted computing bases, encryption, authentication, access control, and physical security. Second-generation security focused on intrusion detection, boundary controls, and content filtering. Third-generation security will take the revolutionary step that will allow systems to operate through attacks and provide real-time notification of large-scale coordinated attacks. The 3GS is made up of a number of component programs that all seek to advance their objective to enable 3GS.

One of these component programs is the Cyber Panel program. It seeks to provide theater-level capabilities to help defend mission-critical information systems by monitoring them for signs of cyberattack and by allowing operators to manage the operation of system security and survivability features to avert or counter developing attack situations. The Cyber Panel approach is to create and validate architectures, algorithms, techniques, and tools that contribute to the ability to identify coordinated attacks, assess system health and mission-relevant attack effects, and choose and carry out effective security and survivability posture changes, either proactively or in response to the appearance of attacks.

The Organically Assured and Survivable Information Systems (OASIS) program's technology development goals are to conceive, design, develop, implement, demonstrate, and validate architectures, tools, and techniques that would allow fielding of organically survivable systems. The technology products will include architectures for building intrusion tolerant systems from potentially vulnerable components; real-time execution monitors to detect malicious mobile code and prevent damage by, and propagation of, malicious code; error detection techniques and tolerance triggers; error compensation, error recovery, and error response technologies; and assessment and validation methodologies to evaluate intrusion tolerance mechanisms.

The Survivable Wired and Wireless Infrastructure for the Military (SWWIM) program seeks to perform the research necessary for demonstrating how to construct an infrastructure that is both survivable and resilient to digital scans and probes, denial of service, and direct attack by both outsiders and insiders. The SWWIM approach will address topics such as emergent routing systems, capability-based systems, onion routing systems, trust management systems, computational immunology, definition of C4ISR architectural constructs, simple distributed key infrastructures, dynamic name spaces, and service quality enforcement. Fault Tolerant Networks will continue to apply fault tolerance techniques to networks and network components. Dynamic Coalitions will continue to develop multidimensional policy and secure group management techniques.

The Operational Experimentation program's goal is to transfer results of the technology programs to operational theaters in the very near term and to obtain experience with the latest 3GS technologies in an operational setting. The technology programs will feed the Survivable Global Information Grid (GIG) System program as a pathfinder for future DoD survivable systems developments. The Survivable GIG System program seeks to provide defense capabilities against sophisticated adversaries in order to allow sustained operation of mission-critical functions in the face of known and future cyberattacks against information systems. This program will deliver a field-tested prototype Survivable GIG System and an integral monitor and control Cyber Panel. The prototype will demonstrate means to enable the entire Global Information Grid, from applications down to communications infrastructure, (a) to operate through a wide class of cyberattacks and provide continued and correct operation of mission-critical functions; (b) to gracefully degrade nonessential system functionality in the face of attacks; and (c) to reconfigure dynamically to optimize performance, functionality, and survivability. The prototype will also demonstrate the following Cyber Panel capabilities: (a) monitor GIG systems for coordinated attacks, (b) provide the Commander with theaterwide IA status and operational impact of failures/attacks, and (c) provide the Commander with the ability to determine theaterwide courses of action and prioritized responses.

DARPA also plans to begin research on a new program entitled Composable High-Assurance Trusted Systems and has made progress within the Open Source community for obtaining guidance in developing this new program.

DEFENSE CONTRACT AUDIT AGENCY

The Defense Contract Audit Agency (DCAA) is responsible for performing all contract audits for the Department of Defense. DCAA provides accounting and financial advisory services regarding contracts and subcontracts to all DoD Components responsible for procurement and contract administration. These services are provided in connection with negotiation, administration, and settlement of contracts and subcontracts. DCAA also provides contract audit services to other Government Agencies. DCAA Headquarters is located at Fort Belvoir, Virginia, supporting approximately 81 Field Audit Offices (FAOs) and 386 suboffices worldwide, with a total of about 4,350 personnel.

During FY 2000, DCAA has focused heavily on IA, mainly because of the importance that IA has attained within the DoD as it converges on greater dependence on networkcentric operations. The recent "ILOVEYOU" virus attack has also pointed out how vulnerable typical software applications, such as electronic mail, have become and how little effort it takes would-be hackers to inflict damage.

DCAA has taken great steps toward improving and optimizing IA manning and billets. The responsibility for designing, managing, and maintaining DCAA's IA posture has been outsourced to contractors who possess professional certification, along with level-II and -III experience. Upon assignment to DCAA, all new hires, including IT and IA staff, are subject to a background investigation. This policy is not new, but it has been actively pursued in FY 2000. In addition, DCAA has identified personnel to serve in the following key roles: Designated Approving Authority (DAA), Information Technology Manager (ITM), Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), Systems Administrator (SA), Public Key Infrastructure (PKI) Registration Authority (RA), and two PKI Local Registration Authorities (LRAs).

During FY 2000, DCAA has written and revised many of its IA doctrines. The DCAA Information Systems Security Policy was revised in April 2000 to reflect changes in Internet and network technologies. An Information Assurance Vulnerability Alert (IAVA) policy was written to provide instruction, establish roles, and assign responsibilities for DCAA support of the Defense Information Systems Agency (DISA) IAVA process. In addition, a Continuity of Operations Plan (COOP), a Critical Asset Assurance Program (CAAP), and a Certification and Accreditation (C&A) policy were written and developed. DCAA also developed policy documents outlining proper uses of government computers to increase employee awareness, as well as a plan to roll out a new commercial off-the-shelf (COTS) operating system at the desktop level in FY

2001, pending a DoD-recommended security structure for the operating system.

Public Key Infrastructure (PKI) is a key component of successful information assurance efforts. DCAA has been active in this arena. Thirty PKI user certificates were issued during initial testing phases for the Agency, and a plan was developed to deploy PKI certificates to all Agency personnel during 2001. DCAA also developed a matrix of in-house software applications to PKI-enable and install PKI server certificates on all intranet web servers.

DCAA removed unauthorized software from PCs and deployed a COTS antivirus to all PCs to provide better management and oversight of PC viruses. In sorting through the aftermath of the "ILOVEYOU" virus, DCAA identified deficiencies with the e-mail server software: namely, that the use of a certain COTS antivirus for e-mail servers did not prevent them from being infected by the virus. In response to these findings, DCAA installed a COTS WebShield software from the DoD Computer Emergency Response Team (CERT) to block all Visual Basic Script (VBS) and Microsoft Scrap Object File (SHS) attached e-mails, which has protected the server from being hit by any of the "ILOVEYOU" virus variants. In addition, DCAA used a COTS utility to remove the "ILOVEYOU" virus from infected mailboxes.

DCAA planned the major redesign of its wide area network (WAN) to reduce the number of NIPRNET entry/exit points from seven to two. These two NIPRNET entry/exit points will be monitored by a DISA-controlled Intrusion Detection System (IDS) and protected by a DISA-approved firewall. The WAN redesign implementation will take place in the first half of 2001 and will increase the IA security posture of DCAA impressively.

DEFENSE COMMISSAR Y AGENCY

The Defense Commissary Agency (DeCA) is responsible for the planning, marketing, business development, and operation of the worldwide network of defense commissaries. DeCA maintains its headquarters in Ft. Lee, Virginia, with a presence in nearly every state and in 14 foreign countries.

IA Training

DeCA recognized that the first layer of protection in support of IA initiatives was to train its personnel. The first step of the Agency to bring the systems administrators up to varied levels of expertise and competency was to develop individual curricula targeted at various skill levels for UNIX and NT systems administrators. Once these curricula were developed, the systems administrators began to immediately pursue the required training for their skill levels and expertise. To date, DeCA has continued to meet the challenge of training and bringing the systems administrators to the highest-attainable skill levels by the Agency's curricula standards.

In November 1999, in an effort to provide DeCA with the latest IA awareness products, IA awareness training materials were sent to DeCA regions for distribution to the stores, ACSs, and CDCs. The training package included two IA awareness videos ("Computer Security 101" and "Cyber Warriors Digital Battlefield & Info War") and one CD ("Operational Information Systems Security, Volumes I and II").

Patrons shop at commissaries like this one around the world.

DeCA also published the DeCA Systems Security for Password Management Handbook. This handbook documents computer security (COMPUSEC) policy and requirements for password management on computer systems and networks that are in the operations and support phase of their life cycles. It applies to all DeCA personnel, including contractors, who use, operate, or manage DeCA computer systems and facilities. The Corporate Server Team and the Telecommunications Team have responded to network and server-based threats such as the "ILOVEYOU" virus, successfully minimizing their total impact

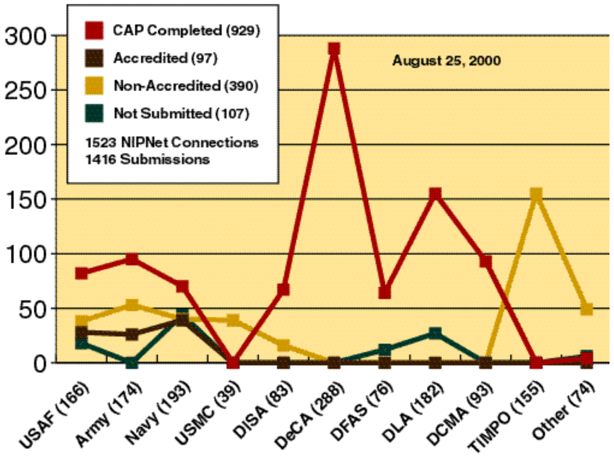


Figure 18. NIPRNet Connection Approval Process

on DeCA's day-to-day operations. DeCA is continuing to acknowledge and update its compliance on all IAVAs. The Telecommunications Team recently completed the NIPRNET Connection Approval Process (CAP), which ensures that DeCA meets the security requirements documented by DoD and that it will continue to maintain the accredited security posture of the network. In the figure, the green CAP completed shows the accomplishments of the agency to date.

In February 2000, DeCA published a Network Security and Firewall Policy, which implements the OSD Network Security Policy memorandum dated 21 December 1999. As part of this effort, DeCA followed the firewall implementation schedule this year. The firewall deployment schedule marks the achievements of DeCA's Telecommunications Team in ensuring that the Agency's network connections are properly routed through a DeCA-approved firewall. Because of the 24x7, worldwide operational schedule, some of the bigger challenges that the Agency faced in deploying the firewall involved working across various time zones and coordinating with the various regions to minimize downtime.

An independent assessment by the Greentree Group recognized a need to monitor both firewall logs and intrusion detection systems and noted a staffing shortage. DeCA will be actively addressing this issue in the coming fiscal year as it constantly seeks improvement in its IA posture.

DeCA Firewall Implementation Milestones

Eastern Region
January 18, 2000 - April 10, 2000

Western Pacific Region
May 15, 2000 - June 2, 2000

European Region
July 6, 2000 - July 21, 2000

Okinawa
September 14, 2000 - September 22, 2000

Figure 19

DEFENSE FINANCE AND ACCOUNTING SERVICE

The Defense Finance and Accounting Service (DFAS) provides the Department of Defense with responsive, professional finance and accounting services. DFAS provides these services under three major business lines: Accounting Services, Military and Civilian Pay Services, and Commercial Pay Services. DFAS employs more than 17,000 personnel.

Fiscal Year 2000 saw the formal introduction of new DoD Global Information Grid (GIG) policy and guidance for implementing a Defense in Depth strategy. The GIG policy provides for the integration of layered protection for all DoD information systems and networks. As a result, DFAS reformulated its Information Assurance Program Plan to address all overarching GIG IA responsibilities necessary to fully implement the Defense in Depth strategy.

Aggressive IA

The Defense in Depth strategy includes implementing the DoD PKI policy and associated guidance, an area in which DFAS remains on schedule. A total of 47 Local Registration Authorities are now equipped and trained, and approximately 4,500 end users have been registered for either a PKI medium assurance or a Class-3 user certificate. Server certificates are installed on all private web servers and are being used to authenticate the servers via Secure Sockets Layer (SSL) protocol. DFAS provided direct support to the DoD common access card program by participating in a smart card pilot project at DFAS Pacific. The DFAS Information Assurance Program Plan incorporates all remaining actions necessary to fully deploy the DoD PKI and common access card programs and PK-enabled applications for the Agency. DFAS corporate IA policy was updated and improved during the year. This major policy rewrite strengthened the management of user access to information systems, increased the authority and independence of information system security officers, and implemented new GIG IA policies within DFAS.

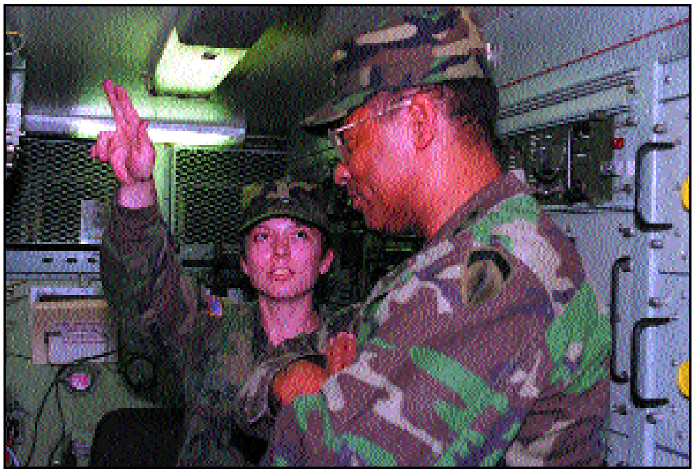
Policy changes also improved the application of the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) to DFAS systems by incorporating a standard format for documentation and procedural guidance to better align DITSCAP activities with system life-cycle phases. During the year, increased management attention to a DFAS-tailored system life-cycle process has yielded improved program compliance with DITSCAP requirements.

DFAS developed and implemented a formal Computer Emergency Response Team (CERT) capability that includes a real-time intrusion detection system for its network. Every midtier platform, router, and server (Novell, NT, and WEB) are now being monitored, in real time, for intrusion attempts. The new DFAS CERT capability also incorporates IA vulnerability alert, incident reporting, and Information Operations Condition (INFOCON) requirements.

IA Training

To enhance education, training, and awareness efforts, DFAS continues to implement its Information Technology/Information Assurance Training and Certification Plan and to remain on schedule to certify every user and systems administrator by 31 December 2000. In addition, all users at every DFAS location have received annual awareness training.

DFAS hosted an intensive conference for Information System Security Managers (ISSMs) in order to review ongoing activities, map strategies, and refocus information assurance priorities, as needed.



A Private First Class explains to her senior officer how the 173 Communications van reads and transmits signals to their direction.

The DFAS Vulnerability Assessment Team (VAT) continued to regularly perform network scans, looking for and correcting weaknesses and vulnerabilities in the network infrastructure.

DFAS also completed Project Bankroll, whereby the Defense Threat Reduction Agency (DTRA), with assistance from the National Security Agency and other organizations, conducted an objective, comprehensive assessment of potential web vulnerabilities, including attempts to exploit them with penetration activities. Recommendations resulting from the assessment will further improve the security posture of the DFAS network and application systems.

DEFENSE INTELLIGENCE AGENCY

The Defense Intelligence Agency (DIA) is headquartered at Bolling Air Force Base in Washington, D.C. It serves to provide timely, objective, and cogent military intelligence to warfighters, soldiers, sailors, airmen, marines, and to the decision makers and policy makers of the U.S. Department of Defense and the U.S. Government.

DIA has successfully implemented protective measures across the three different computing environments of Unclassified, Secret, and Top Secret. To provide efficiency and economies of scale, security capabilities are replicated and managed under a single IA construct. DIA has also installed antivirus software against malicious code and centralized management security software, providing speedy updates of protective software. In its recent security self-assessment, DIA's evaluation of corporate servers and workstations resulted in the identification of vulnerabilities and their mitigation. DIA also reviewed security configurations of commercial software and applied best practices that improved information protection and availability.

Making Use of IA Technology

In securing Agency Unclassified assets, DIA has implemented a layered security approach through the use of firewall technology. The Unclassified firewall is configured to direct incoming traffic to more trustworthy internal systems, to hide vulnerable systems that cannot easily be secured from the Internet, and to log traffic to and from the private network. Secure services can be shared with external organizations through the implementation of an extranet, the semiprotected area segregating DIA's internal, Unclassified network and the NIPRNET.

DIA currently uses network-filtering technology to segregate and protect the DIA internal Top Secret network that is connected to the Joint Worldwide Intelligence Communication System (JWICS). This filtering technology controls the flow of information into and out of the interconnected information system. This results in successful dissemination of intelligence to the warfighter while protecting intelligence information systems deemed critical for operational support in the Intelligence Community.

DIA has implemented an intrusion detection system to provide IA capabilities for monitoring both the JWICS global enterprise and the internal Unclassified infrastructure. The intrusion detection system is a global monitor with deployed sensors providing real-time attack sensing and warning for the Intelligence Community's Top Secret infrastructure. With this capability, DIA has established 24x7 operations to conduct monitoring and provide senior leadership with situation awareness. It also performs the role of coordinating and directing incident response for the Defense Intelligence Community. In addition, the DIA manages the Information Operations Condition (INFOCON) levels and can directly respond on situation awareness, reporting, and to protect against system and network attacks. The intrusion detection system also allows the DIA to identify IA improvements for Communitywide protection and reaction and to provide vulnerability information for the collection and sharing of IA threats.

Aggressive IA

DIA has revised the certification and accreditation (C&A) process for use within the DoD Intelligence Information System Community. The revised process follows the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) methodology described in DoDD 5200.40 and incorporates the information system security requirements of DCID 6/3. Applying this process has given DIA several advantages: First, it establishes a system certification standard across the Intelligence Community, and it replaces the previous documentation requirements with a standardized, fill-in-the-blanks template. The new C&A process also provides cost savings by improving process efficiencies, implementing use of security tools to maximize standards, and reducing travel costs. In doing so, it provides the operational unit with a system configured to meet security requirements after stringent testing in the laboratory and operational environments, and it places responsibility for secure operation on the organization using the system. The awareness caused by this procedure has created more emphasis on security requirements for systems operating in a higher-risk environment.

Making final adjustments to a triple satellite support radio wire on the rooftop of US Embassy, Haiti.

The DoD and the Intelligence Community (IC) embarked on the highly complex task of transitioning the formal messaging system, known as AUTODIN, to the bypass system, using secure Sensitive Compartment Information (SCI) networks. In the Defense Intelligence Community, DIA had the lead IA role for ensuring a secure and interoperable implementation. Termed the AUTODIN Bypass project, this task involved the first-ever transition of all classified message traffic to JWICS. The project was successfully completed, resulting in tremendous IA successes supporting critical information sharing across the enterprise. Here are the highlights of the AUTODIN Bypass project:

- Certification of multilevel secure information systems capable of sending and receiving information across multiple, secure environments
- Full system interoperability with IC and DoD message systems that had not been previously able to send and receive information between each other
- Enhanced IA protection for highly sensitive information traversing the SCI infrastructure

DIA conducted a successful training forum for Information System Security Managers and Officers (ISSM/Os). More than 250 IA professionals attended. Training opportunities on a variety of IA technologies, policies, and briefings from multiple agencies were featured. The forum was a major success, as demonstrated by the response from attendees with regard to presentations, demonstrations, and overall discussions. This training has improved the IA professionals' knowledge and skills.

During FY 2000, DIA has provided intelligence support to IA in various ways. By producing numerous intelligence reports on foreign programs to deal with the Y2K problem, DIA enabled DoD planners to enhance IA on DoD systems in those parts of the world where adequate IA steps had not been taken to protect U.S. interests. By providing threat awareness intelligence products to support DoD systems such as the DISN, Global Command and Control System (GCCS), Global Combat Support System (GCSS), SIPRNET, and others, DIA helped to improve DoD's overall IA posture by supporting needs for security awareness, operational improvements, and improved system designs. By cooperating with USSPACECOM in executing the Computer Network Defense mission, DIA has contributed to developing a reporting system for threats to U.S./DoD networks. These efforts support IA by providing prompt notification of network attacks, thereby facilitating appropriate IA responses.

DEFENSE INFORMATION SYSTEMS AGENCY

Joint Vision 2020 envisions Full Spectrum Dominance, a key component that includes full dimensional protection. Full dimensional protection includes the information domain, which is uniquely subject to asymmetric engagement. In fact, JV 2020 highlights the fact that U.S. forces around the world are subject to continuous information attacks on a daily basis, by both traditional and non-traditional adversaries.

During FY 2000, the Defense Information Systems Agency (DISA) has taken a lead role in providing IA support to the Commanders in Chief, Services, and Agencies. DISA IA support is structured to support the Defense in Depth concept through the implementation of a technical framework that includes the following DISA IA efforts, detailed below under the four categories of the Defense in Depth concept:

- Defense of the computing environment
- Defense of the enclave boundary
- Defense of the network and infrastructure
- Supporting infrastructure

Defending the Computing Environment

IA Pr ogram Management Office Role

The Information Assurance (IA) Program Management Office (PMO) consolidates the acquisition, integration, dissemination, and implementation of IA products and services into the DISA pillar programs (i.e., DISN, DMS, GCCS, and GCSS) and other DoD systems and activities. The IAPMO coordinates with the CINCs, Military Services, and Defense Agencies to determine requirements and develop standardized IA tools, methods, and training/awareness products to support and enhance the overall security posture of DoD information systems.

IA comprises measures and controls that safeguard and protect the confidentiality, integrity, and availability of information systems from unauthorized disclosure, modification, or destruction from such threats as hackers, terrorists, and foreign governments.

DISA employs the Defense in Depth strategy to ensure that information assurance services are implemented across the Defense Information Infrastructure (DII), the seamless web of communications networks, computers, software, databases, applications, facilities, and other capabilities that provide the DoD’s information processing and communications needs.

Information systems are not protected by a single mechanism, but use a layered approach to provide adequate protection against attack (e.g., protect the network, protect the hosts and enclaves, and protect the applications). IA has been integrated into the DISA pillar programs from their inception.

Information Assurance Reviews

DISA provides essential IA support to the Commanders in Chief (CINCs). The CINCs rely on DISA to provide teams of functional experts for comprehensive assessments of their specific enclave vulnerabilities. At the conclusion of these reviews, resolution plans are developed to mitigate vulnerabilities. IA reviews were conducted for eight major CINC headquarters in FY 2000. IA reviews were also extended in FY 2000 to seven CINC Components, including deployed forces in Southwest Asia (SWA). The IA Readiness reviews, system vulnerability assessments, penetration tests, exercise support, IA training, and certification support have increased the security readiness posture of the Department of Defense.

Security Technical Implementation Guides

IA Security Technical Implementation Guides (STIGs) have been developed for every prevalent operating system within the DoD. These guides are the foundation of DISA's review programs and are accessible to all of DoD through a secure website. In FY 2000, DoD Central Design Activities (CDA) participated in the STIG update process to ensure consistent security policy implementation throughout a system's life cycle.

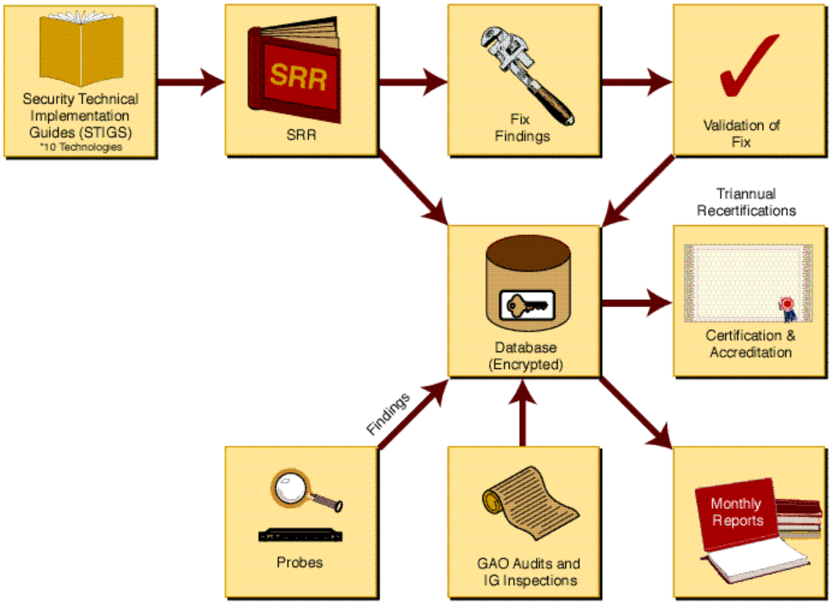

Security Technical Implementation Guides (STIGS)
*10 Technologies
SRR
SRR
Fix Findings
Validation of Fix
Triannual Recertifications
Database (Encrypted)
Certification & Accreditation
Findings
Probes
GAO Audits and IG Inspections
Monthly Reports

Figure 20. Security Technical Implementation Guides are the foundation of DISA 's security r eview programs.

Vulnerability Analysis Assessment

The DISA Vulnerability Analysis and Assistance Program (VAAP) assesses systems and networks for intrusion and security risk vulnerabilities. VAAPs are done every two years for all DISA systems. They promote the fusion of information assurance into all facets of the systems and provide effective identification of vulnerabilities across critical DISA and non-DISA computer systems.

DISA has also developed and implemented the Secret and Below Interoperability (SABI) Joint Vulnerability Assessment Process (JVAP) program, using procedures already established for DISA's Security Readiness Review (SRR) program. The SABI JVAP program includes a set of specific security checks for each SABI guard in use by a CINC. DISA conducted SABI JVAPs at most CINC locations through FY 2000.

The audit server system was developed as a result of SRR findings that auditing was not turned on at the sites. Auditing is turned off because of the huge resource requirements to retain the information in a readable format for evidentiary purposes. The audit server will manage the enormous amounts of data produced by the different security packages. These audit servers will be the data repositories from which data extraction, compilation, trend analysis, anomaly detection, event analysis, and information extrapolation will take place. The amount of audit data captured at the various information technology centers has significantly increased and will continue to grow. To accommodate this growth, DISA fielded a prototype audit server designed to efficiently store and manage audit data in a midtier environment and protect them from loss or damage. The first pilot system was deployed in the second quarter of FY 2000. Targeted sites for FY 2001 include all CINCs and eight DISA Western Hemisphere (WESTHEM) Defense Enterprise Computing Centers (DECCs) and detachments.

Intrusion Misuse Detection System

The Intrusion Misuse Detection System (IMDS) is a system that creates a synthetic network, complete with synthetic hosts and routers, as a tool to detect inappropriate use of Government assets. Simulated services are configured to appear to be running on virtual hosts with unique Internet Protocol (IP) addresses. The IMDS complements a traditional Intrusion Detection System (IDS) by filling in a number of the holes and limitations of an IDS. As a result of IMDS being able to detect inappropriate activity based solely on the destination of network traffic results, the entire set of transactions by an intruder can be collected and identified, rather than just those transactions that meet predefined attack profiles. New exploits and attacks are also handled just as effectively as known attacks, resulting in better identification of attack methodologies and in the identification and analysis of new attack types. Currently, IMDS is deployed to five DECCs, seven CINCs, three Regional Network

Operations and Security Centers (RNOSCs), DISA Field Security Operations, the DoD Computer Emergency Response Team (CERT), and the Air Force Research Laboratory in Rome, New York.

Defending the Enclave Boundary

Intrusion Detection

The networks in the Global Information Grid (GIG) can be likened to a weapon system because they must be monitored, managed, and maneuvered in a way that will allow them to remain protected. Immediate analysis and deconfliction of events is essential for development of proper courses of action, including recovery and reconstitution. Deploying a robust intrusion detection sensor grid, integrated into the global information grid, is essential to protecting the command-and-control networks, services, applications, and infrastructure components.

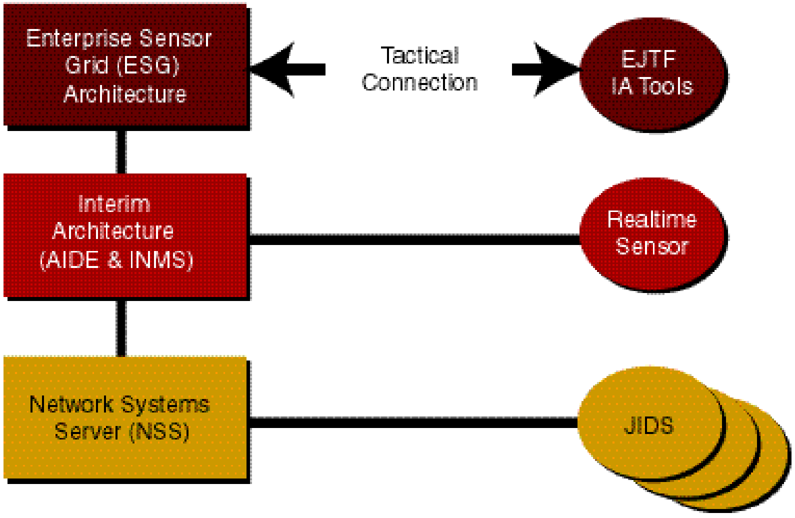

Enterprise Sensor Grid (ESG) Architecture
Tactical Connection
EJTF IA Tools
Interim Architecture (AIDE & INMS)
Realtime Sensor
Network Systems Server (NSS)
JIDS

Figure 21. Enterprise CND Sensor Grid Architectur e

The predominant enclave sensor used by DISA is the Joint Intrusion Detection System (JIDS). DISA monitors approximately 112 NIPRNET and 46 SIPRNET JIDSs at critical DoD network entry points, including Network Management Centers, Standard Tactical Entry Points (STEPs), CINC enclaves, and Defense Enterprise Computing Centers (DECCs). DISA is working with the High-Performance Computing Modernization Program to identify real-time sensor components for high-capacity circuits and is working to develop an Asynchronous Transfer Mode (ATM) network sensor. A network modeling effort to identify strategic SIPRNET locations was completed, and a similar effort has been initiated for NIPRNET. DISA has also started to feed JIDS performance data into the Integrated Network Management System (INMS), thereby further enhancing network situational awareness. The JIDS program provides accurate, timely information that has been compiled, assessed, filtered, correlated, and tailored to the warfighters' current operational situation.

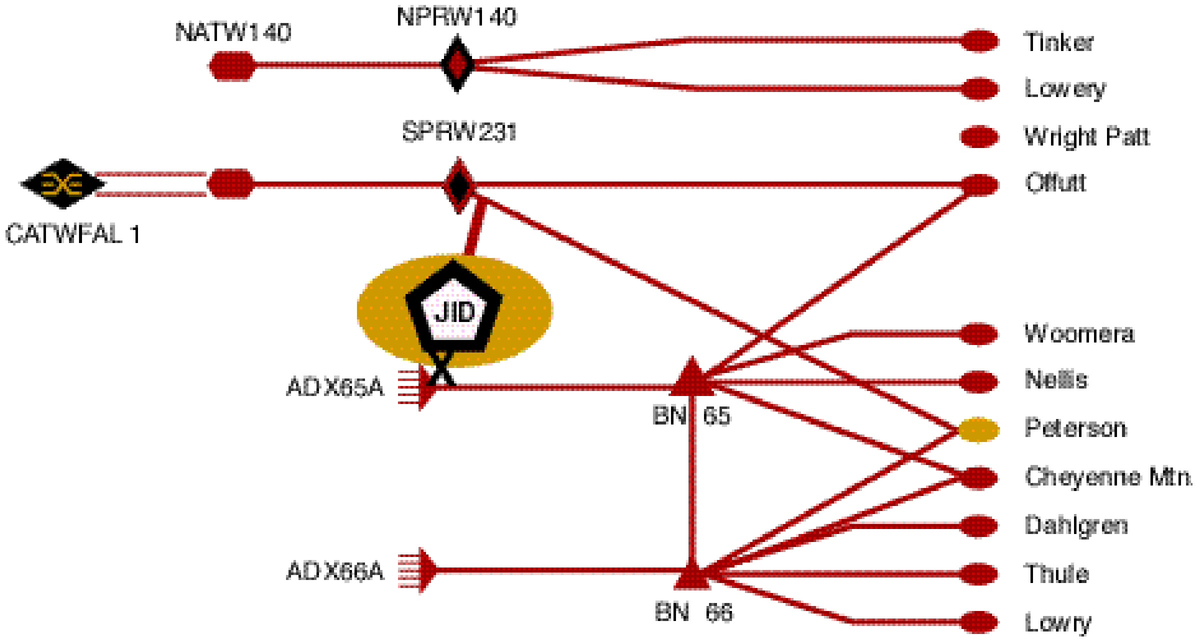


Figure 22. National Representation of JIDS into INMS

U.S. Military Communications-Electronics Board (MCEB) requested an investigation of IA aspects of network management. The Joint Staff J6K and DISA initiated an effort to provide IA components for the Joint Defense Information Infrastructure Control System-Deployed (JDIICS-D). The pilot effort will provide a modular suite of computer intrusion and vulnerability detection tools. The IA components for the JDIICS-D pilot provide deployable tools to monitor and defend the data networks of a USCENTCOM Joint Task Force (JTF) with the following IA functionality over a two-year period: host and network-based intrusion detection, vulnerability scanning, analysis/correlation, and perimeter defense.

IA components for JDIICS-D will provide an initial configurable Defense in Depth IA architecture and sustainment plan for deployed JTFs. Based upon validation of a notional architecture at CENTCOM, the initial architecture will provide a proposed laydown of IA functionality to provide effective and efficient support to a JTF. In addition, a sustainment plan will outline resource requirements, training, help desk, analysis support, and maintenance support for the volatile environment of a JTF.

During FY 2000, development was completed on the JDIICS-D operational test, installation, and implementation plans, and the following four pilot sites fielded and tested the IA components: JTF-SWA, Eskan Village; NCTS, Bahrain; RNOSC, Bahrain; JCSE, McDill AFB, Florida.

Security Le vels

Multiple Security Levels (MSLs) include secure interoperability between networks of differing classifications (e.g., NIPRNET, SIPRNET, and coalition networks) in support of DoD operational and strategic missions through Department C4I programs. DISA has OSD-directed coexecution responsibilities with NSA to oversee and implement the DoD-wide SABI program. DISA provides Command-and-Control Guard (C2G) and technical direction on MSL issues. DISA engineered an upgrade of the C2G, porting the application to the latest B3-Rated Trusted Platform. This upgrade resulted in a 300 percent increase in throughput capability and a 400 percent improvement in the Mean Time to Failure.

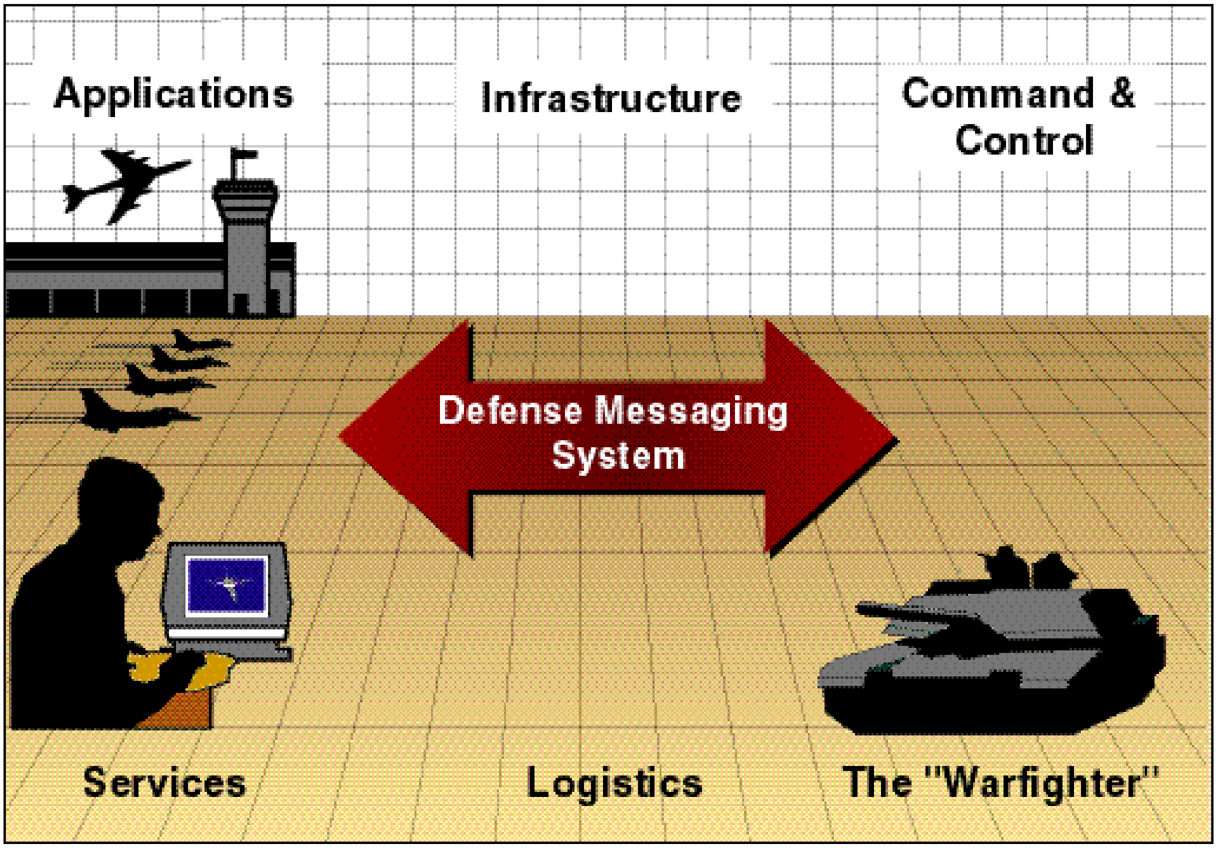


Figure 23. The Global Information Grid

DISA implemented eight C2G system upgrades for C/S/As, including data-filter updates. Coalition interoperability requirements were enhanced through DISA's MSL development and support for CINC North American Aerospace Defense Command/USSPACECOM, allowing additional secure data exchange of Common Operational Picture data for U.S. and Canadian Forces.

Defending the Network and Infrastructure

Asynchronous Transfer Mode Networ k

The Asynchronous Transfer Mode (ATM) network offers an international, standards-based communications infrastructure for combining voice, data, and video services over high-bandwidth backbone circuits supporting both Unclassified and Classified requirements. The Defense Information Systems Network (DISN) ATM network provides for multiple Unclassified and Classified services, allowing tremendous savings in network interface equipment, optimization of local loops, and efficiency and economy in Wide Area Network (WAN) bandwidth costs. The ATM network currently comprises 300 Unclassified and Classified Service Delivery Nodes (SDNs) worldwide and is adding an average of 5 SDNs and 10 user activations/upgrades per month.

DISN ATM network services must provide a trusted infrastructure and an extremely high-bandwidth capability to support the entire DISN customer base at all levels, necessitating improved security posture and sustainment. The network includes DISN ATM Classified service for customers of the CONUS and OCONUS Secret Internet Protocol Router Network (SIPRNET), the National Imaging and Mapping Agency (NIMA), the National Reconnaissance Office (NRO), the Cruise Missile Joint Agency, and DISN expansion support for the

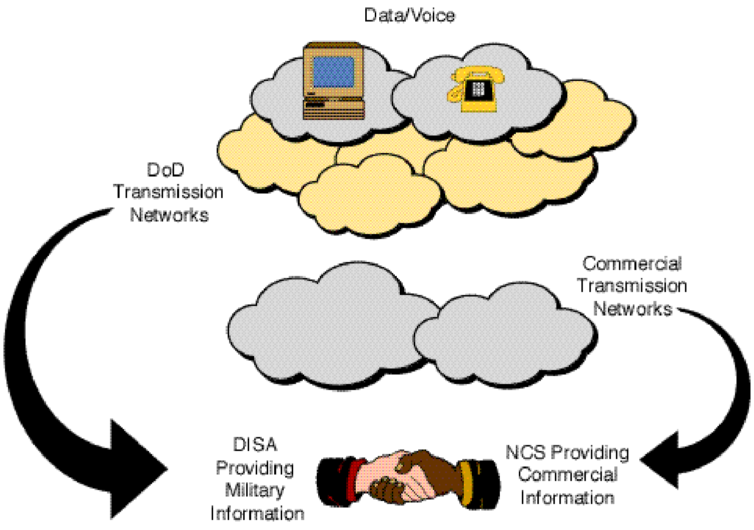

Data/Voice
DoD Transmission Networks
Commercial Transmission Networks
DISA Providing Military Information
NCS Providing Commercial Information

Figure 24. DISN is dependent upon a trusted infrastructur e.

Intelligence Community. Customer projects supported include Predator, Global Hawk, JSIPS, the CINC J2s, Defense Dissemination System (DDS), Bosnia Command and Control Augmentation (BC2A), Global Broadcast System (GBS), Global Command and Control System (GCCS), JOPES 2000, and DoD exercises.

DISN ATM Unclassified customers include CONUS, OCONUS and transoceanic Sensitive but Unclassified Internet Protocol Router Network (NIPRNET), JWICS, DISN Multiplexer, Digital Switched Network (DSN), DISN Video Services Global (DVS-G), and virtual (VCI/VPI) point-to-point ATM transport for DISN common-user waived customers (Tricare, AFSCN, National Guard Bureau, and SCAMPI).

In the ATM Network Risk Management Assessment and Certification, both the Unclassified and Classified ATM networks are required to implement and maintain appropriate security and accreditation measures. To ensure that a high degree of security confidence is sustained, the ATM network must be regularly assessed for all potential threats and shortfalls. Five full-time equivalents (FTEs) are required to maintain the level of risk management activity, monitor abnormal performance and audit trails (including development and update for required documentation), and manage the Connection Approval Process (CAP). A full-time Network Security Officer (NSO) manages all aspects of security and implementation of recommended security improvements for the worldwide DISN ATM networks. The Risk Management Assessment Team will provide ongoing vulnerability analysis, recommend appropriate system upgrades and countermeasures, develop implementation plans, maintain appropriate documentation, and administer the accreditation and connection approval process during implementation of the DISN ATM expansion.

In October 1996, DISA made operational the first wide-area common-user ATM network serving DoD. As the network has grown and evolved, so has the nature of the threats to its stability. To address these threats, DISA developed the IA Architecture for the DISN ATM Services-Unclassified (DATMS-U), which played a key role in the accreditation. DISA performed technology assessments of new ATM security solutions for consideration and implementation into the DISN ATM Management System (AMS) and the DISN ATM Services (DATMS), both Classified and Unclassified. DISA continues to develop methodologies for an ongoing process whereby ATM network vulnerabilities may be analyzed and appropriate countermeasures developed and applied.

In mid-FY 1999, accreditation and risk management assessments of the ATM network began. The results of those activities and requirements published in prevailing DoD and DISA network security regulations require that the ATM network implement secure servers to authenticate and safeguard ATM network management personnel access. Those requirements dictate that one server each for the Classified and Unclassified networks (plus redundant servers) be implemented with Secure ID software to authenticate all access to the ATM network management activities. A total of 12 servers are required, consisting of four servers each per CONUS/PAC/EUR Theater. These servers will ensure that only dedicated ATM support personnel are granted access to the critical network management functions. In addition, the server will maintain a historical audit trail of all logons by date, time, and individual. The initial servers and software licenses were procured and deployed in FY 2000.

Data Networks

The data networks comprise the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET) and the Secret Internet Protocol Router Network (SIPRNET). Since the inception of these networks, DISA has undertaken a number of initiatives to improve their information assurance posture, including the fielding of CISCO PIX firewalls at each of the NIPRNET and SIPRNET network management centers. To ensure the security integrity of each network, DISA has implemented a connection approval process on both NIPRNET and SIPRNET and promulgated procedural restrictions for 1st- and 2nd-level

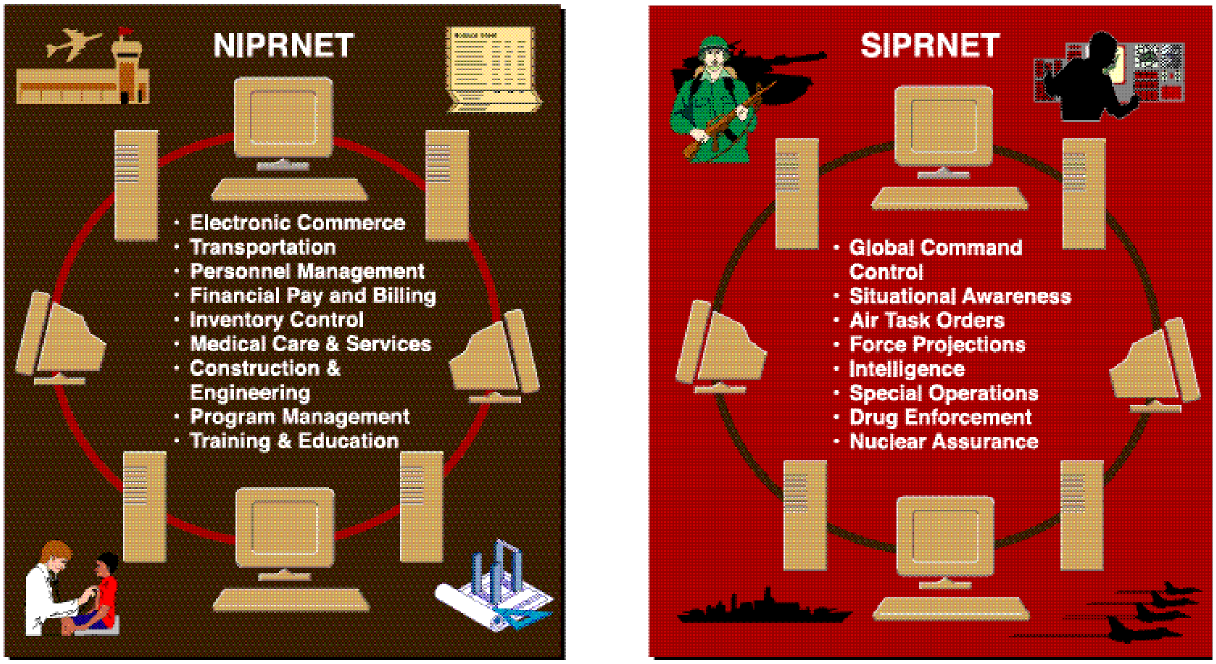


Figure 38. CAP is critical to network security .

domain name servers within the Department of Defense. It has also published a list of 16 restrictions or rules that must be adhered to to ensure the security integrity of the critical infrastructure systems that have been established. Finally, DISA has deployed intrusion detection devices on critical customer access circuits to each network.

The Integrated Tactical-Strategic Data Networking (ITSDN) capability, colocated at the Standard Tactical Entry Point (STEP) sites, is located at various DSCS satellite facilities and provides access to the SIPRNET and NIPRNET for the tactical forces deployed worldwide.

The Connection Approval Process (CAP) program is mandated by the Office of the Secretary of Defense (OSD) and the four Designated Approval Authorities (DAAs). This program is required to validate the security posture of individual customers and the network. Customers submit accreditation documentation for review, both manually and electronically, to ensure that they are properly accredited and are following sound network security procedures. Customers who do not successfully complete the CAP process cannot establish a connection to either network.

The CAP that supports the NIPR/SIPRNET is a critical component in DISA's customer connection process. The SIPRNET CAP is designed to verify that DoD users have completed the required accreditation process and to provide one central repository for network information that would be required if DoD made the decision to electronically disconnect from the Internet. This process is also designed to validate that the network connection belongs to a valid DoD user.

Domain Name Service System

DISA teamed with industry and academia to secure the Domain Name Service (DNS) system. Vulnerabilities that relate to denial-of-service attacks, unauthorized access, and unauthorized alteration of DoD servers are being eliminated. DISA sponsored the development of secured Berkeley Internet Name Domain (BIND) server software and tested and established a standardized Common Operating Environment (COE) configuration management of DNS servers for the DII and identification and authentication for DNS transactions. In May 2000, DISA released a secure version of the DNS software BIND, version 8.2.2P6, segmented on the DII COE for DoD communities.

Project Centaur

The current Centaur Pilot is an existing prototype effort that provides the DoD CERT analysts and incident handlers access to Joint Interconnection Service (JIS) data in the form of Internet traffic statistics, based on TCP/IP header information. As part of DISA's Usage-Sensitive Billing (USB) project, the JIS gateway captures this information. Project Centaur will replace the current pilot effort and will provide additional functionality (e.g., data mining, pattern discovery, and data visualization). The developed system will be scalable so that it can support the projected future increase in data collection and analysis required to support the DoD Computer Emergency Response Team (CERT). Project Centaur provides an improved ability to identify/resolve computer security anomalies. This translates to reduced battle damage and improved support to NCA elements, Joint Staff, CINCs, and the warfighter identification of significant threats to the DII. It also means faster dissemination and implementation of countermeasures and a faster analysis of computer attacks, allowing a more focused response to support the JTF/CND. Project Centaur system requirements specifications have been developed, and the development contract awarded.

Supporting Infrastructures

DoD Public K ey Infrastructur e

In the context of the Defense in Depth strategy, a common, integrated DoD PKI provides a solid foundation for IA capabilities across the Department. The goal of this DoD-wide infrastructure is to provide general purpose PKI services (e.g., issuance and management of certificates and revocation lists in support of digital signature and encryption services) to a broad range of applications at levels of assurance consistent with operational imperatives. Toward this end, DISA has completed two years of pilot study of the Medium-Assurance PKI, having issued more than 60,000 PKI certificates. In July 2000, DISA launched PKI release 2.0, which marks a change in status of the PKI to an operational system called the Class 3 PKI. Version 2.0 adds hardware signing of certificates, using cryptographic boards and Key Escrow/Key Recovery.

In August 2000, the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [ASD(C3I)] signed a PKI policy update mandating a merger of the common access card program and the Class 3 PKI. This merger will become fact in December 2000 when DISA launches PKI release 3.0. Release 3.0 will establish a connection to the DoD's DEERS database, which will automatically create a nine-digit PKI unique identifier for each potential PKI certificate holder. Release 3.0 will also establish the DEERS/RAPIDS Verification Officers as Local Registration Authorities capable of issuing PKI certificates on smart cards that will also be identification cards and building access cards. The PKI policy update also mandated a migration of the Class 3 PKI and current Class 4 PKI to a target Class 4 PKI by 2002. DISA and NSA are currently working to define all aspects of this target PKI.

Defense Messaging System

The Defense Messaging System (DMS) is the messaging component of the Defense Information Infrastructure (DII). It is a flexible, COTS-based application that provides multimedia messaging and directory services.

Security protection for DMS is provided by NSA's Multilevel Information Systems Security Initiative (MISSI) products. NSA ensures the availability of an evolving set of solutions capable of supporting secure interoperability among a wide variety of DoD functions and services within the DII. DMS incorporates NSA high-assurance security products (such as FORTEZZA cards, Certification Authority Workstations (CAWs), and DII guards) as a central part of its security architecture. Implementation of NSA operating system security guidance, automated access controls, security labeling, and In-Line Network Encryption devices will complete a comprehensive, Defense in Depth approach to security for DMS.

Security requirements apply to all DMS subsystems and components. Components are approved for operation in the DMS through a formal accreditation process that is based on the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) for component/system certification. DMS components provide security services such as secure operating systems, confidentiality/privacy of data, integrity, authentication, proof of participation/nonrepudiation, access control, system availability, and audit services. NSA's security products and IA solutions are an integral part of the DMS program. DMS uses, and is dependent on, Class 3 and 4 DoD PKIs. FORTEZZA cards (the DoD Class 4 PKI) and Personal Identification Numbers (PINs) provide high-assurance security encryption and digital signature/authentication services. CAWs are used to generate, manage, and distribute keying material. The CAW also generates and posts user certificates to the DMS Directory. The DoD Class 3 PKI provides software certificates for use by the DMS Medium-Grade Service. The DII Guard provides secure guard services between security domains (e.g., Secret and Unclassified).

In FY 2000, DMS completed installation of 308 CAW 3.1 software packages at all operational sites. DMS completed the initial purchase of CAW 4.2.1 software and installation at DMS labs to begin interoperability testing with DMS 2.2 infrastructure components and initial release 3.0 certificate testing. DMS also provided CAW 4.2.1 software and training tools to the Service schools to enable them to develop Service-specific training plans in preparation for the operational fielding of CAW 4.2.1 in Q1 FY 2001. The CAW 4.2.1 is going to be an important part of the DMS release 2.2 Operational Assessment (OA). In support of the OA, DMS purchased the CAW 4.2.1 for the OA fielding scheduled for Q1 FY 2001. The installation of the High-Assurance Guard (HAG) was installed at two of the six directory guard locations (Norfolk and Gunter), as well as five of the nine CINC locations (USCENTCOM, USSOUTHCOM, USTRANSCOM, USSOCOM, and USJFCOM), to support messaging between the

NIPRNET and the SIPRNET. The installations will be completed at the remaining sites by Q2 FY 2001. The HAG 2.3.1 will be a part of the DMS 2.2 OA.

In FY 2000, DMS has issued two maintenance releases for DMS version 2.1 in FY 2000. Each maintenance release comprises automated security-enabling scripts that lock up the operating systems, based on guidelines produced by NSA and the DISA Field Service Operations (FSO). Each maintenance release has contributed to the Interim Authority to Operate extension for DMS 2.1.

The Development of DMS 2.2 was completed in FY 2000 with 90 percent Security Technical Implementation Guidelines (STIG) compliance and will have completed full testing by early FY 2001. Initial testing by the DISA Information Assurance Program Office (D25), the DISA Field Security Operations (FSO), and the Joint Vulnerability Assessment Team (JVAT) concluded that DMS 2.2 meets security requirements, and an IATO has been granted for operational fielding at the seven Operational Assessment sites and the backbone infrastructure.

High-Assurance Guard 2.2.1 and 2.3.1 have been approved for Unclassified messaging, with attachments between SIPRNET and NIPRNET. Joint efforts from the DISA Information Assurance Program Office (D25), the Navy, NSA, Wang, and LMC produced guard procedures.

In FY 2001, DMS will expand the security features in Medium-Grade Service (MGS), as well as implement MGS at the CINCs, including USEUCOM, USSTRATCOM, and USCENTCOM.

Global Directory Service

The Global Directory Service (GDS) will operate, as appropriate, on both protected and unprotected networks, enabling the DoD to minimize government off-the-shelf (GOTS) developments and leverage existing commercial directory service technology, standards, products, and services. During FY 2000, the GDS established a COTS directory service in a laboratory setting and began to replicate existing directories from within the DoD. Also in FY 2000, the GDS program established the GDS Roadmap and GDS Architecture document, which helps users and vendors to understand the goals, objectives, strategy, and timeline for GDS implementation. In FY 2001, the GDS will become operational on the NIPRNET, providing an initial white-page service and initial asset management.

The GDS will provide a virtual directory service for the Department of Defense. The target GDS will provide an integrated directory infrastructure to support a broad range of commercially based, security-enabled applications and secure interoperability with DoD and its Federal, allied, and commercial partners.

During FY 2000, Global Directories accomplished the following tasks: A Joint Service Working Group that includes members from the CINCs, Services, and Agencies was established for development and prioritization of DoD directory requirements. A draft Global Directories Roadmap was developed that establishes the enterprisewide end-state for the GDS. The roadmap outlines DoD strategy and timelines for the availability of directory capabilities. A survey and evaluation was conducted of available COTS metadirectory products to be used for managing data submitted from various data sources. A prototype of the GDS was developed and demonstrated by merging the data submitted from these data sources, using the metadirectory technology. The GDS pilot demonstrates white-page capabilities and is available via the Unclassified NIPRNET. Currently, the pilot DoD white pages is being deployed to a Defense Enterprise Computing Center. The Global Directories team is completing security assessments and documentation requirements in order to extend service to the SIPRNET in early FY 2001.

CINC IA Representatives

DISA provided direct support to the CONUS CINCs through Information Assurance Representatives. Their role is key to supporting IA coordination, planning, and operations during security readiness reviews, tool deployments, IA exercises, and contingency operations. Security resolution coordination support is also provided to assist with certification and accreditation. Their direct interface with the CINC staff, combined with their coordination with the GNOSC and RCERTs, facilitates DISA's ability to meet the warfighter's requirements.

IA Training and Certification

Information Assurance training support has been provided to security professionals, systems administrators, and system users in UNIX, Windows NT, and Tandem Security for CINCs, WESTHEM, and DISA activities. Twelve Systems Administrator (SA) certification training courses were sponsored, which enabled 238 SAs to secure the necessary training for Level II certification.DISA developed a Tandem Security course for SAs administering and maintaining Tandem operating systems. DISA achieved 100 percent SA Level II certification for SAs of mission-critical Classified and non-Classified systems.

DISA provides Certification and Accreditation (C&A) technical assistance and support to the DoD CINCs, Services, and Agencies. This assistance is provided by a trained staff, providing both on-site and online assistance. The DISA team gave technical (C&A) assistance to 5 CINCs and 21 other DoD activities during FY 2000. Full accreditation or reaccreditation was granted to each activity.

Operations: The Security Office has supported the certification, accreditation, and compliance of DISA and other government systems worldwide on more than 20 reviews. This support has been providing personnel, physical, industrial, COMSEC, SCI, and security reviews, which allow for final or interim authority to operate, based on the overall security posture of an organization, its personnel, and its facilities. To date, either all issues have been resolved, or compensatory measures have been enacted.

DoD Computer Emergency Response Team

The Director of DISA established the Department of Defense-Computer Emergency Response Team (DoD-CERT) to provide operational IA support to the Defense Community. The DoD-CERT is chartered for certain responsibilities, including the response and coordination of computer security incidents, the development and execution of the Information Assurance Vulnerability Alert (IAVA) process, and the management of the DoD-wide virus support and analysis. The DoD-CERT works through these functions both to prevent security incidents and to help restore service after an incident has occurred. It releases security alerts with information on how to avoid incidents. The DoD-CERT is responsible for strategic CND analysis, as well as identification and resolution of DII vulnerabilities on a near real-time basis. Also, it provides vital support to the Joint Task Force for Computer Network Defense (JTF-CND) as its technical component. In this capacity, the DoD-CERT serves an additional role, giving the JTF-CND technical guidance both for daily operations and for exercise planning and execution.

In order to give ample notification and warning, the DoD-CERT maintains several online IA resources available to systems and network administrators in the DoD, as well as Information Operations Cells, Service and Agency CERTs, and information systems security officers. DoD-CERT websites also help disseminate vital IA information, alerts, and tools.

Great progress has been made in the establishment of a Vulnerability Analysis Network (VAN) in the past year. The VAN is necessary to enhance the proactive capabilities of the DoD-CERT and to allow timely testing and evaluation of solutions to vulnerabilities before release. This helps identify and remedy DII vulnerabilities on a near real-time basis and adds the ability to search for vulnerabilities in Windows NT and UNIX-based systems.

The IAVA process received the endorsement of the Deputy Secretary of Defense when the process established by DISA during 1999/2000 was signed into policy. This policy requires all military departments to establish points of contact and distribute alerts and bulletins to the

Figure 26. The IAVA Process

systems administrators, and it requires acknowledgement and compliance reporting. A review of incidents in 1999 shows that most would have been avoided, had recommended compliance activities been followed.

As the Internet and National Information Infrastructure (NII) become larger and more complex, the frequency and severity of unauthorized intrusions into systems connected to these networks become increasingly more serious and continue to grow in number. It is imperative for DoD-CERT to have access to a program that provides a centralized response and coordination facility for global security incident response and countermeasures for threats and vulnerabilities. The relationship established with the FEDCIRC and CERT/CC has strengthened through a series of technical exchanges, working groups, and countermeasure development teams. During the Y2K changeover, the DoD-CERT was identified as the center of continuity of operations for the CERT/CC and will continue to be so into the future. This leverage provides valuable insight into the activities on the Internet and their relationships to activities on the NIPRNET.

Regional CERTS

RCERTs are functionally and organizationally embedded within the five DISA Regional Network Operations and Security Centers (RNOSCs) to provide a comprehensive picture of the health and status of network assets, along with near real-time data on anomalies and intrusive behavior. RCERTs support nine CINCs, DISA WESTHEM, and other DoD agencies to provide incident handling and reporting assistance to develop theaterwide IA reports. The five RCERTs are colocated with the RNOSCs in the Pacific, European, and Central theaters and in CONUS. Currently, the two CONUS-based RCERTs (DECC Columbus and Scott AFB) are transitioning into one consolidated CONUS RCERT. The transition began 15 June 2000 and is scheduled to be completed by 31 December 2000. When it is, it will ease training and infrastructure concerns. Increased manning at one RCERT enables DISA to support near real-time monitoring or a crisis surge in operational requirements. In addition, this will provide an increased ability to establish dedicated customer representatives at one RCERT.

Vulnerability Management

The Vulnerability Management System comprises three components: the Information Assurance Vulnerability Alert (IAVA) website, the Vulnerability Compliance Tracking System (VCTS), and the Security Readiness Review database (SRRDB). These three systems allow the warfighter to track a computer asset's posture relative to emerging (IAVA) and known vulnerabilities (STIG) from discovery through closure. DISA has implemented a web-based version of the SRRDB that allows a quick update and retrieval of an asset's status. DISA also integrated DoD- and C/S/A-unique program management functions into the IAVA and VCTS systems, allowing for reporting of patch information and/or action plans to IAVAs for centrally managed systems. The VCTS was implemented in Washington Headquarters Services (WHS) during the year.

DoD mandated that all CINCs, Services, and Agencies (C/S/As) develop a process to ensure that that command channels, information security offices, and systems/network administrators (SAs/NAs) receive IAVAs. Once an alert is received, SA/NA staff, assisted by the latest technology, acknowledge the IAVA and take corrective action within 30 days. DISA developed the VCTS to address vulnerability management. VCTS is a secure, web-based application that records the notification of responsible parties of IAVAs, catalogs the receipt of IAVAs by asset, and tracks the compliance status of vulnerabilities. VCTS also provides a robust reporting capability, facilitating oversight and reporting for users appropriate to their organizational level. In this manner, a well-honed, multilayered, multifaceted methodology is brought into use. VCTS then provides an automatic feed of IAVA compliance statistics to the IAVA database.

In order to increase the Department's efforts in achieving Information Superiority, the DISA Field Security Operations (FSO) Office has offered the use of VCTS to all CINC HQ, Joint, and subunified Components, as well as to the Services. DISA FSO continues to provide VCTS training, implementation, and operational support to the participating CINCs, as well as OSD activities. Two CINCs are full-fledged operational users of VCTS, and six of the seven remaining CINCs are to be operational next fiscal year. DISA FSO has brought the Defense Messaging System (DMS) into the IAVA age. The PM acknowledges receipt of IAVAs, tests changes against their baseline, and provides a "Fix Action Plan Addressing IAVAs," which is available to VCTS users. DISA FSO is continuing to engage DoD Pillar PMs, as well as individual CINC PMs, in the use of VCTS. This ultimate combination of people, technology, and participation measurably contributes to achieving the Department's IA goals and objectives.

Security Readiness Review Database

Security Readiness Reviews (SRRs) are used to evaluate the IA posture of DoD CINCs, Services, and Agencies. Nine hundred sixty-seven SRRs were conducted in FY 2000. Their findings are tracked in the SRR database. The status of these findings is updated by the users and verified by DISA FSO monthly. The results of these SRRs are used to support site and system C&A recommendations.

The SRR database contains an up-to-date historical record of all security-related findings. As additional systems are reviewed, the number of systems with a security profile in the SRR database is steadily increasing. In addition to being the historical archive of the DISA SRR process, the SRR database provides a variety of reports in support of the DISA IA mission and objectives.

IA Technologies

Automated Intrusion Detection Environment Advanced Concept Technology Demonstration (AIDE ACTD) is a network intrusion detection technology that integrates the outputs of several different intrusion detection sensors. AIDE gathers raw intrusion data from various vendor-unique intrusion sensors and stores them in a database. To enable quick analysis, AIDE normalizes the raw data, filters them to remove duplicates and false positives, accomplishes limited cross-sensor correlation, and presents the data in a readable format.

Final technology demonstrations are being conducted this year, and the final round of spiral development will also be completed this year. In FY 2001, AIDE ACTD will transition to operational status for the Air Force. DISA will use many of the AIDE components and concepts in tools for the JTF-CND and for emerging advanced intrusion detection programs.

The DISA Security Office is considered one of the building blocks upon which the Agency's IA programs are built. This office has the primary responsibility to protect personnel, facilities, and documents, and its IA support crosses all the Agency's pillar programs and missions using the Defense in Depth layers of protection. Examples include the following:

Personnel Security —Despite a DoD security clearance backlog comprising hundreds of thousands of personnel, the Agency experienced a reduction in the time for processing clearance paperwork from 51 days in FY 1999 to 7 days in FY 2000. In addition, during FY 2000, the number of background investigation submissions grew to 1,957, compared with 1,253 in FY 1999. These statistics are extremely critical in comparing DISA against other defense or government agencies in the all-important vetting process—initial and continuous review of military, civilian, and contractor personnel for trustworthiness, truthfulness, and reliability—so that only eligible personnel are hired and kept, thus mitigating the risk to national security. It also ensures that, by being prompt, DISA remains competitive in its hiring process.

Information Security —In October 1999, in light of numerous Automated Information Systems Security (AISS) deviations, the Security Office partnered with the Agency's CIO to reinforce security processes and procedures. The deviations had caused the shutdown or scrubbing of Classified systems and were becoming increasingly costly. This partnership resulted in a Security Stand-Down Day, on which DISA organizations worldwide performed security training on critical elements such as levels of classification, original and derivative classification, classification by compilation, marking, transmission, and sanctions for violations. The AISS violations for FY 1999 and FY 2000 totaled 11 each; however, the traditional security violations have decreased from 27 in FY 1999 to 13 in FY 2000.

Security Awareness and Prevention—Since 1996, the Security Office has performed approximately 135 random entry/exit inspections—with 3,775 individuals inspected. Only three instances of noncompliance have been recorded during this time, with appropriate disciplinary action taken by the individuals' deputy directors. Not one instance of contraband or Classified material has been found. In addition, in FY 1999, two X-ray/magnetometer systems were installed to assist in this process, and two more are being procured. Any visitor or individual that does not have a badge when visiting an X-ray/magnetometer-equipped location must enter (with his or her briefcases, packages, bags, etc.) the X-ray/magnetometer system.

Foreign Visits Program—In FY 2000, the Security Office assisted in processing 158 foreign visits within the National Capital Region (NCR), with an average of three or more visitors for each visit. Of note are the requests for visits/tours of the JTF-CND and GNOSC areas. Because of the unique requirements of each visit, the Security Office has evolved the internal process to include visit approval at the deputy director level, review by a security manager, assignment of an appropriate point of contact, and review/concurrence of the Agency's public affairs officer and deputy chief of staff. In addition, the visitors must be sponsored through appropriate documentation from their embassy. If the appropriate documentation is not forwarded and/or an approval or sponsorship is lacking, the visit is cancelled. The visitors are also vetted for counterintelligence (CI) implications, and any patterns that appear to develop are passed to the Agency's CI Officer.

Joint CERT Database

The Joint CERT Database allows the sharing of DoD intrusion data with the JTF-CND, Service CERTs, the Intelligence Community, and law enforcement organizations. The aggregation of computer network attack incidents allows contributors to see and perform analysis on the aggregated global data, thereby providing a comprehensive DoD-wide IA situational awareness and reporting capability. During FY 2000, JCD version 2.0 was completed, and progress was made toward the development of version 3.0. Benefits to the warfighter include the following:

- Assess the incidents reported by C/S/As and regions individually and cumulatively for their impact on the warfighter's ability to carry out current and future missions
- Identify significant threats to the DII and develop, disseminate, and implement countermeasures to these threats in a timely manner
- Coordinate the response actions taken by the Regional and Service Incident Response Teams
- Identify and resolve computer security anomalies that affect the DII's ability to support NCA elements, Joint Staff, CINCs, and the warfighter

Common Operating Environment

The Defense Infrastructure Common Operating Environment (DII COE) provides the software foundation on which the majority of all DoD command-and-control systems (GCCS, GCSS, GCCS-M, MAGTE C4I, MCS, and others) are built. DISA refined security assessment tools and guidance for securing command-and-control hosts and applications, improved DII COE security services, increased application and segment security lockdown configuration, developed a Security Services Architectural Framework for PKI, and implemented DoD's IAVA process for DII COE software components. The security enhancements to the COE significantly improve the warfighter's capabilities to operate command-and-control systems in a hostile information warfare environment.

Information Superiority Situational Awareness

Between the concepts of Information Operations, Information Assurance, and Network Operations (NETOPS), there exist a relationship and interdependency. DISA initiated the Information Superiority Situational Awareness (ISSA) project to investigate the feasibility of addressing the warfighter's need for a COP of NETOPS. The FY 2000 phase of ISSA was to develop a concept exploration prototype capability to collect relevant information from extant network, system management, and IA reporting databases. It also relates the data to warfighting business processes and provides the warfighter (CINC and CJTF) with situational awareness of the potential impact to critical warfighting processes. The purpose of the concept exploration prototype was to investigate the technical feasibility of the effort, as well as the adequacy of data in extant databases.

I Assure

The IA Information Technology Capabilities Contract (I Assure) is a seven-year indefinite delivery/indefinite quantity contract that was awarded in July 2000. This contract provides a vehicle through which DoD and other Federal services and agencies may contract for IA professional services and IA-enabling technologies. The I Assure contract is the primary contract support vehicle for the IA program and the future funding vehicle for the DISA programs.

IA Education

DISA continued to develop and disseminate IA education, training, and awareness (ETA) products. This OASD(C3I) activity provided classroom training to CINC, Service, and Agency personnel. It also gave them interactive multimedia, computer-based, and web-based training and awareness to support certification of systems administrators and users. In FY 2000, the DISA IA Program Management Office distributed almost 100,000 copies of IA training and awareness products to be used by Service schools and training organizations, by unit trainers to support IA training and awareness in the field, and by individuals seeking to enhance their IA knowledge. CyberProtect, for example, has been incorporated as a formal part of the curriculum into the IO course offered at the Air War College, Maxwell AFB. Operational Information System Security is fully integrated into CNET's NS&VT course. Since FY 1998, nearly 225,000 IA training and awareness products have been distributed.

DISA IA ETA initiatives included production of Secret and Below Interoperability (SABI) web-based training (WBT) product, UNIX Security for Systems Administrators WBT, Information Operations (IO) Fundamentals WBT, and Windows NT Security for Systems Administrators WBT. Web-based IA ETA products to be completed by the end of CY 2000 are Defense in Depth and Certificate

Authority Workstation (CAW). DoD INFOSEC Awareness is being updated to address insider threats, computer ethics, and new threats such as distributed denial-of-service attacks.

In addition, two core, hands-on classroom courses on Windows NT Security for Systems Administrators and UNIX Security for Systems Administrators, supporting DoD systems administrator certification, were updated and expanded with the participation of subject matter experts from USSPACECOM, USEUCOM, USSOUTHCOM, and USSOCOM.

As part of its franchise efforts, IPMO provided train-the-trainer support, combined with DITSCAP and ISSO/ISSM platform training, to USEUCOM, USAFE, USCENTCOM, USSOCOM, DITC-Japan (7th Fleet, 7th AF, and Guam), and U.S. Forces Korea (8th Army and 7th AF). This training brought current INFOSEC/IA training to the CINCs and their theaters of operation.

DISA IPMO products are being distributed throughout the Army National Guard and the Army Reserves. They are a key element of DISA's DoD outreach activities to other Departments and Agencies. NASA has adopted many of the products and given funding to support the development of others, in partnership with the IPMO.

Under PDD 63, Critical Infrastructure Protection, the DISA IPMO products are supporting Federal outreach to state and local law enforcement through the NIPC, to IA educational centers of excellence through NSA, and to the private-sector energy industry through DoE.

DEFENSE LOGISTICS AGENCY

The Defense Logistics Agency (DLA) is a logistics combat support agency whose primary role is to provide supplies and services to America's military forces worldwide. Its 28,600 skilled and dedicated civilian and military staff work around the clock, in all 50 states, in about 27 countries, and at more than 500 sites located close to its customers and suppliers.

Defense in Depth Strategy and Implementation

DLA recently reorganized to provide essential military logistics support for the twenty-first century warfighter. The new millennium brings dramatic changes to the future battlefield and to the way that DLA conducts operations across the entire spectrum of war. In this new environment, the DLA motto, "To provide the right item, at the right time, at the right place, and at the right price every time," means that DLA must have better, faster, best-value logistical solutions for the U.S. military forces to achieve victory. DLA is working toward this goal largely through electronic commerce and the use of strategic partnerships with industry so that DLA can become more effective, agile, and responsive. As a result, IA is becoming a critical component of everyday business to ensure availability, integrity, authentication, confidentiality, and nonrepudiation of DLA information and information systems.

Along these lines, DLA's newly formed Information Operations Directorate, J-6, consolidates the Agency's information technology activities to enhance electronic commerce, logistics support systems, and document automation in support of military logistics. DLA is improving its IA posture through the application of DoD's Defense in Depth strategy.

Knowledge Management and Training

During FY 2000, DLA assumed an active role in increasing Agencywide awareness of the importance of IA within its operations. DISA provided IA-related compact discs and videotaped presentations that were distributed throughout DLA. DLA contracted with DISA to provide introductory IA courses to its field activities. DISA was also contracted by DLA for development of an IA training plan for the Agency. IA training plan completion is planned for the first quarter of FY 2001. To discuss current concerns/issues, DLA also established an Education, Training, and Awareness Working Group, with representatives from DLA Headquarters and field activities.

DLA also coordinated the efforts of its IA professionals and established knowledge-sharing forums. Workshops were conducted for Systems Security Authorization Agreement (SSAA) facilitators and risk assessors and for Information System Security Managers and Officers (ISSMs/ISSOs). Regular IA video-teleconferences were established with DLA ISSOs from the field. DLA sent key IA staff members to the Fourth Annual DoD Information Assurance Workshop, held at Hampton Roads, Virginia, in February 2000.

DLA is publishing supplemental IA policy and guidance to ensure that IA procedures are carried out consistently and in a standardized fashion in accordance with DoD directives.

Security Enhancements

The DLA Computer Emergency Response Team (CERT) took great strides this year in enhancing the DLA security posture.

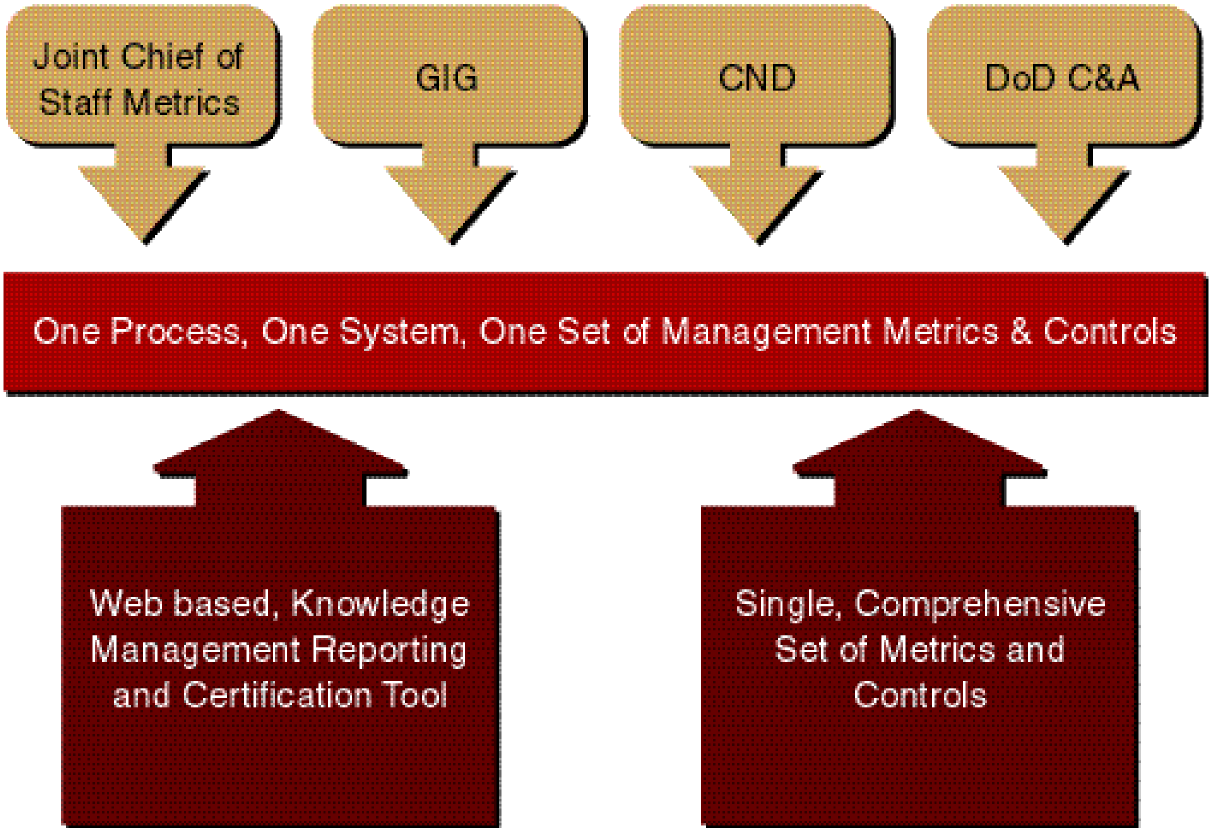

Joint Chief of Staff Metrics
GIG
CND
DoD C&A
One Process, One System, One Set of Management Metrics & Controls
Web based, Knowledge Management Reporting and Certification Tool
Single, Comprehensive Set of Metrics and Controls

Figure 26. Program Integration Reduces Costs, Reporting Burdens and Improves IA

The DLA CERT conducted vulnerability scans of the DLA web server infrastructure. The scans produced a great deal of useful and directly applicable information. In addition, the DLA CERT completed deployment of a more secure version of Domain Name Server software and began deployment of more secure versions of electronic mail software. The DLA CERT also stepped up its operations to a 24x7 basis during the Y2K transition. Other initiatives being pursued during this time are in the following areas:

- DLA required its field activities to verify that antivirus products are deployed both at the desktop and at the server level and that antivirus signatures are kept up to date.
- DLA required its field activities to verify that auditing is enabled on all servers and workstations and that clocks on audited computers are accurate.
- DLA directed its field activities to ensure that routers under their control are configured to reject directed broadcasts and to reduce spoofing by applying ingress and egress filters on the routers.
- The DLA CERT significantly improved DLA field organizations' responsiveness to Information Assurance Vulnerability Alerts (IAVAs).
- The DLA CERT obtained access to its field infrastructure and deployed a set of centrally monitored intrusion detection systems (IDSs).

The CERT also completed deployment of firewalls to DLA's Distribution Depots. The Defense Distribution Center (DDC) has 24 Distribution Depots located throughout the United States, in Germany, and Japan. The Depots store 4.3 million stock numbers in 500 million cubic feet of storage space and process more than 25 million transactions annually. Clothing and textiles, electronics, industrial, general and construction supplies, subsistence, medical materiel, and the military services' principal end items are among the commodities for which the DDC is responsible. Of the 24 depots, 10 are protected by firewalls operated by the host Military Service, and 14 depots, requiring a total of 16 separate firewalls, are protected by DLA.

DLA began deploying new IA tools, including vulnerability scanners and secure virtual terminal software, to DLA field activities. It also started to use PKI servers and user certificates in conjunction with several DLA web servers.

Process Development and Improvement

DLA initiated the DLA Information Assurance Performance Review (IAPR) process and conducted IAPRs on 11 of its field activities. These reviews included both on-site and remote assessment efforts and covered many aspects of IA, including IA administration, certification and accreditation, training, network security incident response, IAVA program, and recovery capabilities. The

IAPRs were a highly successful tool that allowed DLA and its field activities to conduct an accurate assessment of their IA weaknesses and goals and to use the results to improve their IA posture. DLA is continuing to refine the IAPR process. Current plans require sites to be reviewed every three years.

Certification and Accreditation

DLA developed an innovative, two-pronged approach to documenting system and site certification and accreditation. This approach uses a powerful set of web-based tools that integrate four overriding DoD IA policies into a single programmatic and system focus. They enable application of a single program and process to ensure that DLA fully complies with DoD's Defense in Depth strategy and that it has adequate IA protection mechanisms in place. The integrated process implements all required DoD-mandated controls at the site and system levels to ensure timely and cost-effective certification and accreditation for DLA's extensive systems inventory. This program integration reduces costs and reporting burdens and improves IA. It combines to provide one process, one system, and one set of management metrics and controls focused on mitigating DLA corporate threats and risks.

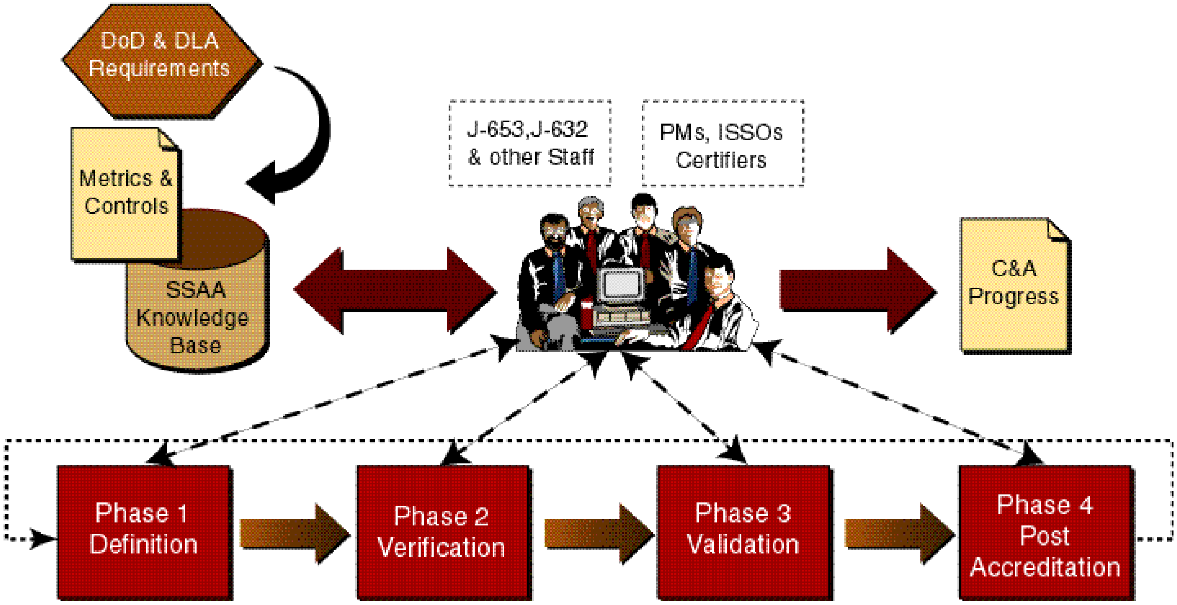


Figure 27. DLA Implementation of C&A

The IA SSAA Help Desk continues to provide assistance to the several DLA sites' and systems' Certification Authorities, ISSOs, and Program Managers (PMs). This assistance ranges from providing the SSAA Template and Plan of Actions and Milestones (POAM) to answering questions regarding the completion of certain SSAA tasks.

Certification and Accreditation Database

DLA developed a C&A tracking database that is used to monitor the progress of each system, network, and website through the accreditation process. It also produced a DLA Certification and Accreditation Project Plan, which currently provides a schedule for completion of the C&A within the Agency by July 2002, with recertification being conducted before, during, and after that date, as necessary. The table shows DLA's projected dates for completion.

DEFENSE SECURITY SERVICE

The Defense Security Service (DSS) provides all security services for the DoD. These services include personnel security investigations, industrial security services, security education and training, and counterintelligence. DSS has implemented the IA program to closely reflect the Defense in Depth strategy. DSS uses a combination of commercially available products and services from the public and private sectors in a balanced approach in order to ensure the integrity and availability of its systems.

DSS maintains a full-time staff of security professionals whose sole responsibility is the execution and oversight of its Information Assurance program. The IA staff at DSS serves as the CIO's advisor on all matters pertaining to Information Assurance to ensure the highest level of protection for the information that it is responsible for.

USING DEFENSE IN DEPTH

DSS uses a layered approach to enclave boundary protection. A router at the perimeter of DSS's network is the first point at which a security mechanism is installed. Filtering rules are installed on this router to block unnecessary and dangerous protocols.

The second layer of defense in DSS's enclave boundary protection architecture is a set of COTS firewalls installed at the perimeter of DSS's internal network. Firewalls are used to limit access to DSS's internal network to specific users, to limit user access to specific predetermined assets, and to log all network connections. See Figure 28, below.

Constant monitoring maintains the integrity of the router at the perimeter of DSS's network and its firewalls. In addition, the firewalls are monitored so that the latest software patches that address newly discovered security vulnerabilities are installed.

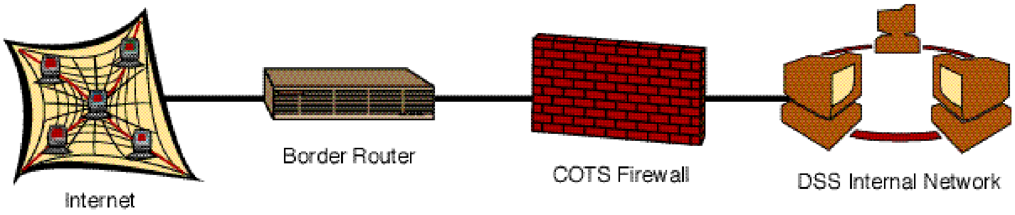


Figure 28

DSS maintains a Virtual Private Network (VPN) capability between trusted users who reside outside of DSS's network and its firewalls. The VPN gives these users a protected channel to access to DSS's information assets. This capability ensures that sensitive Unclassified information is not compromised during transmission to trusted users. See Figure 29, below.

For the virus detection capability, all users are required to install virus-scanning software and maintain updated virus signature files for the affected software. In addition to virus-scanning software, DSS maintains a user awareness program that educates users about security alerts regarding e-mail, attachments, and other IA-related matters. These countermeasures are effective, as evidenced by the fact that several viruses (such as "ILOVEYOU") had a very minimal impact on DSS operations.

Three areas make up the supporting infrastructure portion of DSS's IA program:

(1) DoD PKI,

(2) intrusion detection sensors, and

(3) incident response capability.

DSS maintains a DoD PKI infrastructure that provides users with the ability to digitally sign and encrypt electronic communications within DSS and between DSS and its corporate partners. This capability ensures the integrity and confidentiality of DSS's electronic communications. To date, more than 90 percent of all users within DSS have DoD PKI certificates and have received training on how to sign and encrypt e-mail.

DSS maintains intrusion detection sensors at strategic points in its network. Intrusion detection sensors

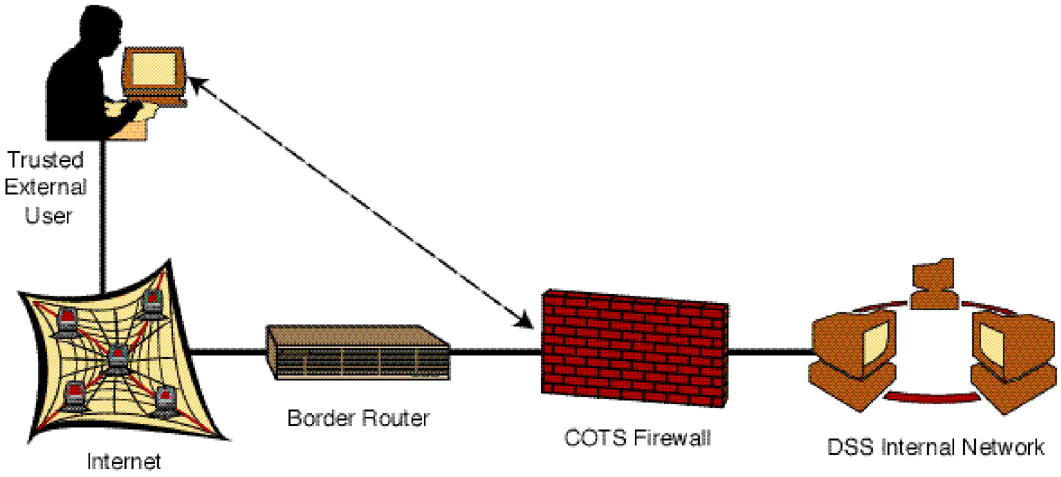


Figure 29

are used to monitor the network for suspicious activity and to warn security administrators when anomalous behavior occurs. Real-time network activity monitoring ensures that security administrators respond to attacks quickly, limiting damage.

DSS maintains an incident response team in order to address network security incidents. DSS's incident response team tracks anomalous network behavior, tracks new vulnerabilities identified in the private and public sectors (e.g., CERT, DISA ASSIST), reports network incidents to the proper officials, and serves as DSS's focal point for Information Assurance Vulnerability Alerts (IAVAs).

IA Accomlishments

During FY 2000, DSS had several significant IA accomplishments:

- Increasing the number of intrusion detection sensors throughout the corporate network from 2 to 12, thereby greatly increasing the ability to detect attacks in progress
- Regularly warning users about proper use of electronic mail (This effort resulted in minimal damage from several viruses that occurred during the year, such as the "ILOVEYOU" virus.)
- Initial implementation of a hierarchical Information Systems Security Officer (ISSO) structure that will allow DSS to achieve a 100 percent compliance rating, with the requirement to report to DISA the number of systems susceptible to specific IAVA alerts
- Initial implementation of a program to accredit all the NIPRNET connections that DSS maintains
- Initial implementation of a program to accredit all Automated Information Systems(AIS) at DSS, using the DoD Information Technology Security Certification and Accreditation Program (DITSCAP) methodology

DSS experienced many IA challenges during FY 2000. Funds were insufficient for fully executing the IA program. Qualified security professionals who could fully execute the IA program were already difficult to hire and retain in sufficient numbers. In order to overcome this challenge, overguidance budget submissions were provided in an effort to increase the funding available to the IA division.

DEFENSE THREA T REDUCTION AGENCY

The Defense Threat Reduction Agency (DTRA) is headquartered in Dulles, Virginia, with eight operating locations around the world. Its responsibility is to reduce the threat to the United States and its allies from nuclear, biological, and chemical (NBC); conventional; and special weapons. It achieves its mission through the execution of technology security activities, cooperative threat reduction (CTR) programs, arms control treaty monitoring and on-site inspection, force protection, NBC defense, and counterproliferation (CP). It also supports the U.S. nuclear deterrent and provides technical support to the DoD Components on matters relating to weapons of mass destruction (WMDs).

IA Efforts

DTRA continued to focus considerable attention on IA during FY 2000. Program emphasis began shifting from the development of interoperability between the systems of the legacy organizations to implementing a DTRA-unique IA program. Progress has been made in implementing a sound Defense in Depth strategy. Since DTRA is primarily an end user of information technology (IT), the majority of its efforts are concentrated on protecting the local enclave.

The DTRA has developed a very basic, integrated Computer Network Defense (CND) program comprising a small corps of government personnel and augmented by contractor support. This group coordinates or provides a full scope of CND services within the limitations of available resources. These services include policy development, Identification and Authentication (I&A), system auditing and monitoring, system Certification and Accreditation (C&A), and IA training.

During FY 2000, DTRA established an Information Assurance Panel (IAP), under the authority of the CIO and chaired by the Chief of Security Office, to provide guidance and oversight to all Agency IA activities. Each Component of the Agency, responsible for a portion of the IA program, is represented. Panel representatives coordinate with the IA policy-making arms of the Office of the Secretary of Defense and the Joint Chiefs of Staff to review and integrate approved guidance into DTRA programs. The panel also sends representatives to Department IA working groups and subcommittees. In addition, the panel has established several working groups to address Agency IA initiatives such as remote access, PKI, palm top computing policy, and IA training. The creation of this panel has led to greater coordination and integration in implementing the DTRA IA program.

IA efforts at DTRA have continued to grow and expand. A paramount concern in these efforts has been to ensure that only properly cleared individuals, with verified need to know, are granted access to DTRA systems and networks. IA personnel also verify that user passwords are in conformance with DoD standards for composition and periodic change and that users with remote access requirements receive the appropriate software, access tokens, and training to ensure the protection and integrity of the system. Whenever a user is suspended, terminated, or voluntarily departs DTRA, system access is immediately disabled.

View of a Minuteman missile inside its hardened launch silo.

IA Awareness

During FY 2000, DTRA also expanded its system auditing and monitoring efforts. In addition to quarterly vulnerability analysis and penetration testing, upgrades to Agency firewalls provided increased protection from intrusions and greatly enhanced the monitoring capability. The introduction of the Joint Intrusion Detection System (JIDS) on the enclave boundaries has also provided a wealth of new data on attempts to gain entry to the enclave. In conjunction with JIDS installation, the DTRA IA program established a relationship with the DoD Computer Emergency Response Teams (CERTs) in Washington, D.C., and Columbus, Ohio, for limited round-the-clock monitoring support. In the event of a penetration attempt or virus attack during nonduty hours, personnel in the DTRA Operations Center will notify appropriate IA and IT team members. In addition to DoD CERT support, daily in-house reviews are conducted on firewall and antivirus audit logs. Future initiatives now underway will enhance this monitoring capability further by providing analytical tools for audit reduction, pattern analysis, and anomaly identification. The DTRA IA team is exploring ways of expanding this capability into a 24x7 CERT if funding and manpower become available. The DTRA IA program has also established a relationship with the Counterintelligence (CI) Community through in-house CI assets. A relationship is also in place with the Defense

Criminal Investigative Service for law enforcement support as required. All suspected intrusions/penetration attempts are reported to the CI and Law Enforcement Communities, as appropriate.

Also during FY 2000, DTRA accelerated its system certification and accreditation (C&A) efforts, despite difficulties in finding and retaining qualified personnel to perform the work. Generally, two to five contractors are available and actively working on C&A activities at any given time. As a result of Y2K preparations and visits to various Agency elements, 95 systems have been identified as requiring C&A work. During the year, 48 systems were documented and granted Interim Approval to Operate (IATO) or full accreditation. It is expected that all systems will be documented and granted IATO or full accreditation by the end of FY 2001.

In response to DoD mandates, DTRA began working on moving from its existing computer-security user-awareness training program into a full-blown IA training program that meets all regulatory requirements. The Agency has defined and is currently implementing a training program for all systems administrators, security personnel, and users. As available training resources are limited, DTRA is focusing on developing self-paced, computer-based training. Level one systems administrator training will be finalized and implemented by the end of FY 2000. Level two and automated user training will follow and are expected to be implemented in the first half of FY 2001.

Making Use of Technology

Another area in which DTRA has taken an active role is the integration of IA procedures and processes into DTRA Research and Development (R&D) activities. The goal is to ensure the protection of confidentiality, integrity, and availability of information through policy enforcement. Policy enforcement mechanisms can be broadly categorized as protection, detection, and restoration. Protection mechanisms include broad deployment of two factor authentication systems for access to restricted networks and servers, introduction of PKI solutions to allow for roaming credentials, and boundary protection through the use of firewalls and access control lists. Early research is also underway for developing secure multicasting techniques that will allow the resource distribution of files, applications, battle plans, and other important data through secure information dissemination. Protection is further enhanced by close attention to well-prepared systems configurations. A number of detection mechanisms are deployed, including antivirus scanners at enclave boundaries, as well as on all servers and workstations.

A near real-time intrusion detection system provides alerts for system scans and intrusion attempts. Activity logs are maintained and reviewed for suspicious and malicious activities. Throughout the Agency, IA personnel regularly monitor industry websites for the latest information on new and current exploits, software vulnerabilities, and malicious code attacks. Finally, careful attention is paid to the restoration of systems in the event of a disaster. Redundant Array of Independent Disks (RAID) configurations are extensively used for data storage. System-level backups are performed on a regular basis. Critical hardware components are maintained on uninterruptible power supplies. A continuity of operations plan that will allow for data replication, load sharing, and multiple points of presence with the DTRA R&D Community is currently in development.

The DTRA also made progress in expanding its IA supporting infrastructures during FY 2000. Initiatives were launched for both an IA Vulnerability Alert (IAVA) program and a PKI implementation program. An annual staff assistance visit program was also started, in conjunction with other security disciplines, to take the IA program out to the Agency community.

The DTRA IAVA program was established in compliance with regulations to disseminate alerts, warnings, and bulletins to appropriate IA and IT personnel throughout the Agency. Each DTRA system and network point of contact to be notified in the event of an alert is identified. Each Component has been tasked to identify an inventory of systems for entry into the IAVA database. The DoD CERT alerts, warnings, and bulletins are acknowledged and disseminated to the contact list, as appropriate. In addition, the DTRA IA team conducts a daily review of industry IA sites, including the CERTs, antivirus vendors, news sources, and hacker information sites, as well as vendor sites for key hardware and software. Information bulletins are prepared and disseminated, as appropriate.

During FY 2000, DTRA formally launched a PKI implementation program. Requirements for DTRA to conform to regulatory guidance have been identified. The greatest challenge faced by the program is expected to be the PK-enabling of applications. Other accomplishments during the fiscal year included the identification and training of Registration and Local Registration Authorities (RAs/LRAs). Computer workstations for the RAs/LRAs were recently procured with funding from the DoD PKI Office. This will allow for the issuance of server certificates, as well as the limited issuance of certificates to individuals for testing. The pace of further program implementation is uncertain because it remains unfunded.

DTRA also launched a security staff assistance visit program that includes representation from the IA staff. Besides presenting an opportunity to learn more about Agency activities and requirements, the program allows the early identification and correction of vulnerabilities and deficiencies and provides an opportunity to conduct end-user training. The IA program has also leveraged this initiative to gather information for system accreditation efforts.

While DTRA has made considerable progress in implementing Defense in Depth, a number of challenges remain ahead. The DTRA IA program remains 100 percent funded with Agency discretionary funds. Any further expansion of DTRA IA efforts will have to come from funding specifically earmarked for IA programs. Expansion is further hampered by an industrywide shortage of fully trained and qualified IA personnel, making it difficult to retain the competent personnel currently employed.

NATIONAL RECONNAISSANCE OFFICE

The National Reconnaissance Office (NRO), headquartered in Chantilly, Virginia, designs, builds, and operates the nation's reconnaissance satellites. Its mission is to enable U.S. global information superiority in times of war as well as peace. NRO is responsible for the unique and innovative technology, large-scale systems engineering, development and acquisition, and operation of space reconnaissance systems and related intelligence activities needed to support global information superiority.

NRO has made significant improvements in its IA posture during FY 2000. Before January 2000, the CIO staff at NRO constituted primarily a Y2K office. After the Y2K rollover, the office was reorganized to address IA issues that had been overshadowed by the Y2K effort. An IA and cybersecurity group was created and given a charter to spearhead an enterprisewide IA program.

In an effort to do this properly, NRO is working with the Software Engineering Institute, Computer Emergency Response Team (CERT) Coordination Center (CC), and is exploring working relationships with the Naval Postgraduate School, Purdue University, and the University of Idaho. All these institutions are IA Centers of Excellence, as recognized by the National Security Telecommunications and Information Systems Security Committee. IA discussions have been held with mission partners, as well as several contractors and various other commercial organizations known for their exceptional IA implementation experience.

NRO has developed an IA policy, with an IA Management Plan (IAMP) that outlines IA roles and responsibilities anticipated to be released in the near term. The IAMP will include dozens of individual programs, procedures, or processes that implement narrowly defined IA functions such

A Delta II rocket on the launch pad prior to launching a Global Positioning System satellite into orbit.

as Public Key Infrastructure (PKI), Defense Messaging System (DMS), or IT system Certification and Accreditation (C&A). The C&A process has already been developed, and a malicious code protection program is now being generated.

It is anticipated that by this time next year, the IA program will be in full swing, with the IA policy and IAMP fully implemented across NRO and supported by its contractors and mission partners, with the goal of becoming an IA Center of Excellence in the U.S. Government.

NATIONAL SECURITY AGENCY

The National Security Agency (NSA), headquartered in Fort Meade, Maryland, coordinates, directs, and performs highly specialized activities protecting U.S. information systems and producing foreign intelligence information. A high-technology organization, NSA is at the forefront of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the Government.

NSA leads the Federal Government in implementing and developing the Defense in Depth (DiD) strategy. NSA's achievements improved the protection of its infrastructure and developed/implemented solutions to the Department's DiD layered IA strategy.

AGGRESSIVE IA

In defense of the NSA infrastructure, NSA established the NSA Public Key Infrastructure (PKI), improving identity on its networks by providing certificates to servers and users. Internally, it improved protection of NSA's web servers by issuing policy mandating the use of PKI-based access control. NSA enhanced its ability to respond to network-based security incidents by establishing the NSA/CSS Information Systems Incident Response Team (NISIRT). To increase the security baseline of all of its systems, NSA created the NSA/CSS Information and System Certification and Accreditation Process (NISCAP). This process is based on a directive issued by the Director of Central Intelligence for accreditation and the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

To comply with IC and DoD security guidance, NSA updated security policies. It established the NSA policy for periodic,

A soldier fires an M-249 Assault Weapon while another ensures the targets down range are being engaged.

mandatory training for information system security. All personnel with an account on NSA's networks successfully completed the first cycle of training. NSA also established and made operational a certification program for systems administrators to improve their security knowledge.

NSA's FY 2000 DoD-wide IA activities focused on implementation of the Department's DiD IA strategy. While strategy and tactics are evolving in conjunction with the changing network environment, the provision of IA builds on NSA's long history of protecting data and communications. NSA provides the leadership, products, and services needed to allow customers to protect national security and sensitive information in information systems, pursuant to Federal law and national policies. The Agency also provides technical support to the Government's efforts to incorporate IA into the Defense Information Infrastructure (DII) and National Information Infrastructure (NII).

During FY 2000, NSA served its customers by assessing their needs, creating IA technologies, delivering and sustaining solutions, and supporting their defensive information operations. NSA promoted security across the DII and NII through policy and standards work, through efforts in public advocacy and education, and through influencing commercially available security technology. Enabling customers to protect and defend cybersystems, NSA developed and supported a variety of products and services and conducted ongoing IA research to help develop the next generation of solutions. These solutions included the technologies and tools necessary for a layered DiD strategy and tools for defensive information operations, such as intrusion detection, automated data reduction, and modeling/simulation tools.

In the area of defending the network and infrastructure, advanced research continued on secure communications and network management capabilities. Solutions for wireless communications were focused on upgrading the security functionality of several commercial wireless products and improving the interoperability between wired and wireless systems. Under wired technologies, efforts were directed at developing additional capabilities for the Secure Terminal Equipment (STE) and improved interoperability between the STE and secure narrowband digital solutions. Other efforts were directed toward development and upgrade of secure inter-networking technology equipment and product development and upgrade activities in the areas of special applications technologies, space technologies, and combat applications.

Regarding enclave boundary defense, NSA focused on the use of IA components to add a layer of protection. The target environment for enclave boundaries includes service layer networks, modem connections, and laptops that may be connected remotely to different service networks. Efforts continued toward laying the groundwork for a comprehensive program to increase the security functionality and capabilities of enclave boundary products through participation in the development and upgrade of various commercial firewall and guard products. In addition, a product comparative list was developed to assist customers by describing the functionality and security characteristics of a growing number of available enclave boundary security products.

An important role of the computing environment is to provide identification and authentication, confidentiality, integrity, and nonrepudiation services for general use to the end user. NSA's efforts in this category included development of application functions such as secure messaging, file transfer database access, file encryption, web access, and electronic commerce. In the area of cryptographic engines, modules, and tokens, NSA continued the development of server tokens, including a Personal Computer Memory Card International Association (PCMCIA) token/modem to meet the requirements of a high-assurance remote access system. Additional efforts focused on the development of protective technologies to be used in the creation and deployment of host-computer components and end-user devices. Research efforts were aimed at developing state-of-the-art secure computing technology, as well as applying technological advances to the areas of cryptography, network security engineering, authentication, and end-system (workstation) security.

Activities in the supporting infrastructure areas included a set of interrelated efforts designed to provide security services to enable and manage a broad scope of IA technology solutions. A major focus was the continued development and upgrade of NSA's Electronic Key Management System (EKMS) and its supporting equipment, and initial efforts toward the development of a DoD-wide PKI. The PKI efforts centered on the development of required updates to the DoD PKI Roadmap, Certificate Policy, and Implementation Plan.

The other major focus is on attack sensing, warning, and response. In this area, NSA operated a 24x7 activity that issued threat warnings, attack alerts, and bulletins; conducted diagnostics on attacks against national security systems; and provided this information to U.S. Government Departments and Agencies. Under NSA's effort to develop a DoD detect-and-respond infrastructure, activities included the successful filtering and analysis of an initial flow of data from forward-deployed sensors to isolated protocols of interest. In addition, functional requirements for this attack sensing, warning, and response system were established, and the first suite of protection profiles was completed. Other infrastructure activities included the development of a web-based graphical user interface containing key information needed by network intrusion analysts, such as analyst tools and technical information.

IA Methodology

NSA devoted much effort to develop a systems security methodology that includes a systematic set of interrelated processes for addressing the user's security needs. Toward this end, a coordinated version of the Information Assurance Technical Framework (IATF) was released that aligns with the Department's DiD strategy and provides architectural guidance for the wireless and tactical technology areas. In addition, nine IATF forums were hosted to educate U.S. Government employees and contractors in current IA plans and technological capabilities. Personnel working in this area also participated in several other DoD and Governmentwide working groups, promulgated the DiD strategy, and assisted in solving customers' IA problems. Protection profiles, documenting 16 reusable IA solutions, were completed, making optimum use of IA development resources to meet the security needs of a broad base of IA customers.

NSA provided system security engineering and consulting services to a variety of U.S. Government customers, helping them to identify and implement appropriate IA solutions in their networks and information systems. NSA analyzed government- and commercially developed IA products to advise customers appropriately regarding the proper application of security solutions. NSA also offered security assessments to DoD and U.S. Government customers. In order to make the identification of security solutions more accessible to its DoD customers, NSA adapted the IA Exchange architecture to provide on-line customer access to NSA's IA solutions and services. In addition, NSA experts developed technology forecasts to guide the efforts of NSA, Defense Research Projects Agency (DARPA), and other DoD components performing IA research.

To better inform IA customers of the capabilities of commercial IA products, NSA and the National Institute of Standards and Technology (NIST) created the National Information Assurance Partnership (NIAP), which accredits commercial laboratories to validate IA commercial products within the internationally accepted Common Criteria (CC) structure and publishes the resulting test data. Beyond these efforts, NSA worked collaboratively with IT industry leaders at improving the IA functionality and assurance levels of their products.

IA Operations

The DiD strategy identified the need for a global cryptographic infrastructure that supports key, privilege, and certificate management and enables positive identification of individuals using network services. In this area, NSA continued its activities in Security Management

Infrastructure Operations (SMIO), which include production of the paper and electronic codes and keys required to support IA solutions through material generation, distribution, and management. NSA also arranged life-cycle and depot-repair services, operated a help desk, provided online support for user self-help, maintained configuration documentation, and provided field troubleshooting for government-developed solutions. Other activities included completion of the EKMS Phase 4 requirements analysis, development of a Phase 4 Backend Test Plan and Procedures document, operation of the FORTEZZA PKI Operational Center in support of the DoD's high-assurance (Class 4) PKI requirement, and near completion of a prototype vector generation system.

An officer prepares to transmit imagery using the IMMARSAT system.

NSA's Defensive Information Operations (DIO) effort focused on the ability to detect rapidly and react to attacks and intrusions, as well as that of enabling IA situation awareness and response in support of DoD missions. Toward these objectives, NSA DIO efforts developed tools for security analysis of networks, partnerships with Federally Funded Research and Development Centers (FFRDCs) to advance understanding of new intrusion detection capabilities, and in-depth analysis and evaluation of several DoD networks. In addition, DIO's Active Network Defense program focused on completion of the development and testing of prototype verification modules to enable the detection of anomalies in the Internet Control Message Protocol (ICMP) and the File Transfer Protocol (FTP). A joint analysis workstation was developed, with the capability for network analysts to share information, to parse and sort data, and to perform key word searches across multiple operating system environments. The Operations Readiness program provided flexible, integrated, and tailored support to the warfighter through a continuum of vulnerability assessments, evaluations, and red-teaming activities. Participation in these activities helped identify improvements in hardware, software, policies, and procedures to better protect U.S. systems.

NSA recognized that security education, training, and awareness were essential to a successful IA program. In support, training programs and course materials for current and candidate Information Systems Security Engineers (ISSEs) were developed. Internally, NSA provided training and development activities for NSA's employees to improve their system engineering capabilities, to improve communications, and to keep researchers and systems administrators current on IA technology and security issues. To assist IA R&D personnel, NSA supported technical/scientific laboratory employees assigned to NSA by providing a productive work environment and necessary travel funds and supplies. The Agency also established a Systems Security Engineering Certification Program (SSECP), ensuring that graduates performed a full spectrum of systems security engineering services.

NATIONAL IMAGER Y AND MAPPING AGENCY

The National Imagery and Mapping Agency (NIMA) is headquartered in Bethesda, Maryland. NIMA is responsible for providing timely, relevant, and accurate imagery, imagery intelligence, and geospatial information in support of national security objectives. Major operating locations are in Washington, D.C., Northern Virginia, and St. Louis, Missouri. Support and liaison offices are located worldwide. NIMA leads the Imagery and Geospatial Community (IGC) in designing, acquiring, deploying, maintaining, and continuously improving the United States Imagery and Geospatial Information Service (USIGS).

IA Training

NIMA has widely supported training programs to increase IA awareness among its employees and to train and educate key personnel in IA technologies. These personnel participate in a variety of required and optional IA education, training, and awareness programs that range from short self-study modules to conferences and seminars. NIMA has also developed and implemented a web-based Public Law 100-235 training module. By accessing online training modules, NIMA personnel can complete this required training at the time that is most convenient to them. Lastly, NIMA has reached all DoD milestones for Information Systems Security Officer (ISSO) and Systems Administrator (SA) training. One hundred percent of key personnel have been trained.

Through the development of the Information Systems Security Officers (ISSOs)/Information Systems Security Managers (ISSMs) Professionalization Plan, NIMA has certified ISSOs and ISSMs assigned to systems and sites for which they are responsible. NIMA's Designated Approval Authority (DAA) and Principal Accrediting Authority (PAA) have been fully certified in DITSCAP and DAA basics. All eight members of its Incident Management Team (IMT) have been fully certified as Information Warfare Officers by the Air War College. The NIMA IA Certification and Accreditation Program has accomplished the following:

- Accredited 131 systems
- Certified 140 systems (9 pending accreditation)
- Certified 5 international program sites
- Delegated DoDIIS certification authority for D/DIA accreditation
- Certified 10 DoDIIS.
- Assisted in standup of the NIMA Industrial AIS Program and facilitated consolidation of NIMA's collaborative computing efforts

NIMA accreditation activities also had an active role in the Intelligence Community (IC). Representatives participated in development of the National Intelligence Certification and

Accreditation Process (NICAP) and in the development of DCID 6/3 instructions for IC contractors. NIMA developed the Streamlined Security Plan that was adopted as the model for all IC Industrial Site Security Plans. NIMA played an active role in NSA's ATM risk assessment, in the development of IC Interdomain transfer policy, and in the development of the IC SABI process.

The Agency has established an IA program that provides Agency-level representation to National Security Telecommunications and Information Systems Security Committee (NSTISSC), the Defense-wide Information Assurance Program (DIAP), and the Intelligence Community's (IC's) Information Assurance Policy Board (IAPB). NIMA's IA Program Manager or an alternate regularly participates in NSTISSC, DIAP, and IAPB forums and apprises NIMA's CIO and other leaders and managers of Federal civilian, DoD, and IC IA program plans, activities, and issues.

The NIMA IA Program Manager chairs monthly meetings of its Information Assurance Steering Group (IASG), which comprises managers responsible for subprograms. It receives guidance and direction from the NIMA CIO's Executive Council, establishes program goals and objectives, assigns responsibilities, and monitors program status. Most important, the IASG serves as a management mechanism for coordinating the work of the following 10 subprograms managed by IA professionals throughout the Agency:

- Policy and Procedures
- Critical Infrastructure Protection (CIP)
- Certification and Accreditation (C&A)
- Intrusion Detection System/Computer Network Defense (IDS/CND)
- Information System Security Officer/Manager (ISSO/ISSM)
- Public Key Infrastructure (PKI)
- IA Training and Awareness
- Incident Management Team (IMT)
- System Security Engineering (SSE)
- Computer Security (COMSEC)

An Army Captain gives a mission brief to his troops while in the field.

NIMA personnel are working with OSD(C3I) on the development of a DoD directive on Information Assurance and a DoD instruction on Information Assurance Implementation. NIMA personnel supported DoD analysis of mobile code threats and helped develop the mobile code policy. They formed a NIMA Mobile Code Forum (MCF) to understand and discuss the impact of mobile code on NIMA and sent representatives to DoD mobile code forums. NIMA shares the concern of the DIAP leadership regarding the increased use of mobile code. NIMA will continue to work within the program to implement management and technical controls that will help to mitigate the risks associated with this increasingly popular technology. Working under DoD and IC policy and guidance, NIMA is developing a policy to govern the use of mobile code within USIGS. NIMA was recognized by the Office of the Secretary of Defense for its participation in the DIAP mobile code initiative.

Advancing IA At NIMA

NIMA is developing an IA Business Plan to better track IA needs, requirements, capabilities, shortfalls, and improvement strategies. A key component of the plan is the use of IA Readiness metrics. In addition, NIMA's Incident Management Team (IMT) has developed and fully implemented a Corporate Antivirus Strategy Plan, which encompasses techniques and procedures for automatic update of virus definitions in antivirus software on NIMA-owned laptops. When personnel with laptops log-on to NIMA networks from remote sites, the antivirus definitions are checked and automatically updated, if necessary. Laptops used for remote logon to NIMA networks were assessed for vulnerabilities, and NIMA is now analyzing the results of the laptop inspection in order to recommend laptop policy to the NIMA CIO and to schedule needed updates to ensure that these devices are properly configured with the latest antivirus software and virus definitions.

Aerial view of the runway at a Port Au Prince airport in Haiti.

NIMA established an Information Assurance Engineering Review Board (IAERB) to manage IA-related engineering and technical issues. The IAERB identifies problems and issues, assigns actions and due dates, reviews proposed solutions, and directs implementation.

NIMA has also established an Intrusion Detection Team responsible for the detection and the prevention of unauthorized access or exploitation of NIMA information and information systems. This team also provides CND operations, including support to the NIMA Incident Management Team (IMT) - Computer Incident Response Team (CIRT), which comprises eight people. The IMT-CIRT works with the DoD CERT in assessing incidents and determining the best response strategies. Because of these efforts, the impact of the "ILOVEYOU" virus and other major malicious-code threats have been seriously reduced and, in some cases, altogether avoided. In recognition of their achievements, Lieutenant General James C. King, Director, NIMA, awarded to the IMT-CIRT a Meritorious Unit Citation.

NIMA is actively engaged with DIAP partners in developing IA Readiness assessment methodology and readiness metrics. NIMA held a two-day, off-site metrics conference in May 2000, during which the group defined the initial set of IA metrics. NIMA participated in the July 2000 DoD metrics workshop and the September 2000 meeting of the DoD IA Readiness Working Group. NIMA concurs with DIAP leadership on the importance of developing a capability to measure the assurance benefits that they receive from program investments and will support the DIAP in developing uniform measurements and collection processes.

NIMA has developed a draft USIGS Goal Security Architecture Framework (UGSAF) that provides both goal architecture and a roadmap for its accomplishment. The UGSAF provides guidance for specifying and implementing specific USIGS affectivity security architectures at interim points in the overall implementation of USIGS. The UGSAF also addresses the security challenges of systems using the Internet and distributed object technologies, as well as IA focus on availability, integrity, authenticity, confidentiality, and nonreputability. It forms the basis of the security component of the evolving USIGS architecture.

Making Use of IA Technology

During the year, NIMA personnel tested, evaluated, and added to the NIMA antivirus software baselines for Windows NT and Macintosh OS. The Software Management System (SMS) provided 52 weekly and 18 out-of-cycle virus definition update operations to more than 4,000 For Official Use Only (FOUO) workstations. The SMS installed the following IA-related configuration changes during the past year to desktop computers on NIMA’s Sensitive But Unclassified (SBU) network and Secret Collateral Enterprise Network (SCEN):

- Logon banners with DoD warning notices
- Reconfiguration of the Local Administrative Group on each machine for security reasons
- Planned delivery of password-protected screen saver to each workstation
- Installation of security patches, Y2K patches, and version upgrades

NIMA's Intrusion Detection Team has selected a commercial Intrusion Detection System (IDS) to perform host-based and network-based intrusion detection. The hardware will include servers for traffic detection and analysis for the SBU and SCEN networks. NIMA is currently working with the vendor to implement the tool on the SIPRNET, Internet, and Gateway Services locations.

NIMA's System Security Engineering (SSE) subprogram is concerned with the design and acquisition of security capabilities for protection of the United States Imagery and Geospatial Information Service (USIGS), which is NIMA's enterprise system for support to the Imagery and Geospatial Community (IGC). This subprogram has formed a USIGS Security Engineering Integrated Process Team (USE IPT), which holds monthly meetings, identifies issues and actions needed to resolve them, and tracks the accomplishment of assigned actions.

NIMA supports both the DoD and IC PKIs. NIMA has established a PKI project team (led by a project manager), which comprises registration personnel and systems engineering support personnel. Team members are actively involved in both the DoD and IC PKI technical working groups. NIMA has also developed a PKI Project Management Plan. The plan describes NIMA's schedule, which is aligned with DoD policy, as well as project requirements such as documentation, standards, personnel, funding, training, and risk mitigation. In support of the ongoing PKI efforts, NIMA established a PKI Engineering Review Board, which is led by the PKI project manager and comprises representatives from the registration, systems engineering, testing, Internet/intranet/extranet, and firewall areas. The board tracks and resolves engineering issues.

NIMA has identified 3 Registration Authorities (RAs) and 11 Local Registration Authorities (LRAs), located throughout NIMA facilities in the Washington, D.C., area and in St. Louis, Missouri. RAs and LRAs have attended the appropriate training and are accordingly certified. To help streamline the certification process, NIMA developed a standard operating procedure for registration and issuance of DoD certificates. NIMA established an e-mail pilot and issued 50 user and 10 server certificates. E-mail certificates are used to digitally sign and/or encrypt messages between pilot members, as well as between three other DoD Components and one contractor. NIMA began issuing certificates for private web servers on its extranet and enabled them for server authentication through Secure Sockets Layer (SSL). Ten RA/LRA workstations have been installed in the Washington, D.C., area and seven in St. Louis, Missouri, and are being used in the e-mail pilot.

The NIMA-specific applications that will be PK-enabled [such as U.S. Imagery and Geospatial Information Service (USIGS) applications, extranet, and human resource applications] have been identified. NIMA plans include using digital certificates with DoD applications such as Defense Messaging System (DMS), Defense Travel System, Standard Procurement Systems, and Wide Area Work Flow. PKI training and awareness efforts include PKI information on the NIMA intranet. NIMA's PKI web pages contain information on user support, PKI contacts, and PKI and IA training, as well as links to other PKI and IA resources. Two instructional briefings have been posted on the intranet: "End-User PKI Instruction" and "Using PKI Certificates." There is also information about PKI in NIMA's Public Law 100-235 training.

NIMA continues to lead the Intelligence Community in compliance with Critical Infrastructure Protection (CIP) and Continuity of Operations (COOP) planning. The NIMA Continuity Planning Division (MSC), in the Mission Support Office (originally established as the Critical Information and Infrastructure Protection (CIIP) Division) integrates the planning and program management functions associated with Critical Infrastructure Protection (CIP), Continuity of Operations (COOP), Business Continuity (BC), and Disaster Preparedness (DP) planning. MSC's integration of emergency planning was the model the DoD used for preparation of a draft DoD Instruction for Integrated Continuity Planning.

During the past year, MSC has helped NIMA accomplish a number of critical milestones. NIMA participated in several external disaster preparedness, risk management, and business continuity training events. MSC has helped NIMA sites upgrade their Disaster Preparedness Plans by conducting training assessments and preparing and delivering emergency exercises in conjunction with the Disaster Control Staffs at each NIMA site. These exercises helped validate existing plans and improve training levels. Below is a sample of the type of exercises performed and where they have been done:

- Barricaded Suspect - Bethesda, MD and St. Louis, MO
- Bomb Threat - Reston, VA
- Loss of Utilities - Washington Navy Yard, Washington, DC

NIMA has played an active role in both the Intelligence Community and DoD COOP programs. NIMA's Continuity of Operations Plan, originally signed in August 1999, has been continually updated and has recently been redistributed throughout the agency. NIMA COOP planning is performed in conjunction with the Intelligence Community COOP, DoD

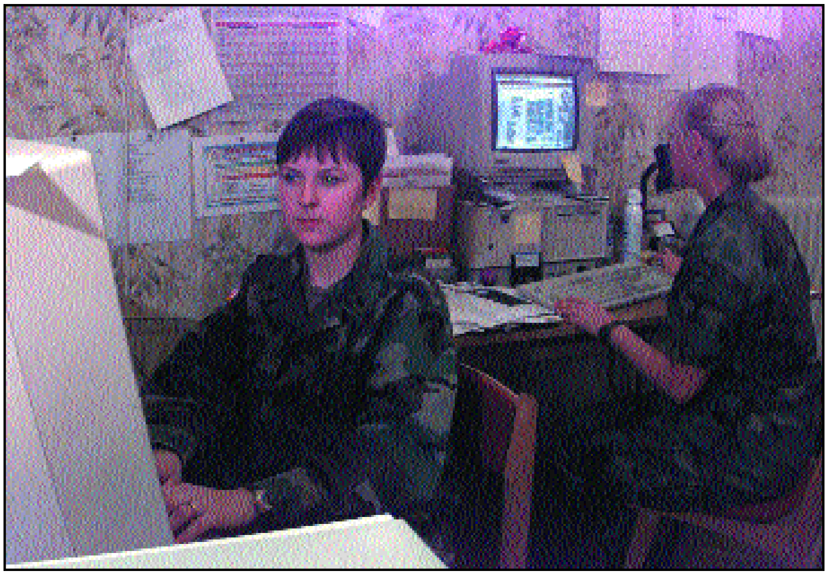
COOP, and FEMA COOP working groups. MSC has supported IA exercises for NIMA's Incident Management Team and participated in Intelligence Community and DoD COOP exercises.

ARMED FORCES INFORMATION SERVICE

The American Forces Information Service (AFIS) is a field activity of the Office of the Assistant Secretary of Defense for Public Affairs. The AFIS mission is to provide high-quality news, information, and entertainment to U.S. forces worldwide in order to enhance unit and individual readiness, quality of life, and morale. AFIS trains public affairs and communications professionals and provides a full range of communications services to support the informational needs of commanders and combat forces, their families, reservists, retirees, and others interested in learning about DoD. AFIS also manages DefenseLINK, the official DoD public website.

AFIS facilities include its headquarters in Alexandria (Virginia); the Defense Information School (DINFOS) at Ft. Meade (Maryland); the Armed Forces Radio and Television Broadcast Center (AFRTS) in California; Visual Information Centers in California and Pennsylvania; the Television-Audio Support Activity in California; and the Stars and Stripes newspaper offices in Washington, D.C., Europe, and Japan.

To achieve its mission goals, AFIS undertakes activities that require extensive interaction with the public and commercial entities through the Internet, even during heightened Information Operations Conditions (INFOCONs). Consequently, much of the FY 2000 IA activity centered around the need to achieve a level of IA that would permit AFIS to access the commercial Internet and the military portion of the Internet (NIPRNET), even if DoD had to disconnect the NIPRNET from the Internet. The broad AFIS goal is to establish a unified IA program that meets or exceeds all DoD IA requirements, conforms to the shared DoD IA vision, and ensures that the AFIS IT system fully supports its mission.



Specialists type out their stories on their computers.

AFIS users are now completing the OSD-developed, web-based IA training module. Internal security and system use policies and one-on-one training augment this training for new employees. To further enhance the knowledge of its in-house staff, AFIS contracted for in-house technical security training for many of the Information Resources Management (IRM) personnel. In addition, specific training was targeted for particular members of the IRM team to help them better accomplish their jobs. AFIS will extend this training to the IT staff at all AFIS sites in FY 2001.

AFIS-HQ contracted with the service arm of a leading IA vendor to conduct a security gap analysis and to provide recommendations on the basis of its findings. DINFOS added a full-time security contractor to assist with infrastructure improvements and assigned a person full-time to initiate the DITSCAP process. At AFIS-HQ, an additional person was hired and responsibilities shifted to allow more time to address security issues.

AFIS applied best-practices systems administration to maintaining hardware and software and performing backups. The AFIS-HQ IRM staff fully documented their systems and implemented configuration management improvements to ensure that future changes are documented and tested. Lessons learned from this activity will provide guidance in creating policies for the field activities in FY 2001.

IA Technology

AFIS has begun DoD PKI implementation, and the AFIS Registration Authority and Trusted Authorities have been identified. Secure Sockets Layer (SSL) using DoD PKI certificates has been implemented on several web servers at two sites within AFIS.

To facilitate the eventual connection to the NIPRNET, AFIS-HQ staff created and implemented a network architecture that conforms to guidance in DoD CIO Memo No. 6-8510. This architecture separates internal, publicly available, and remote access networks with a firewall controlling access between them.

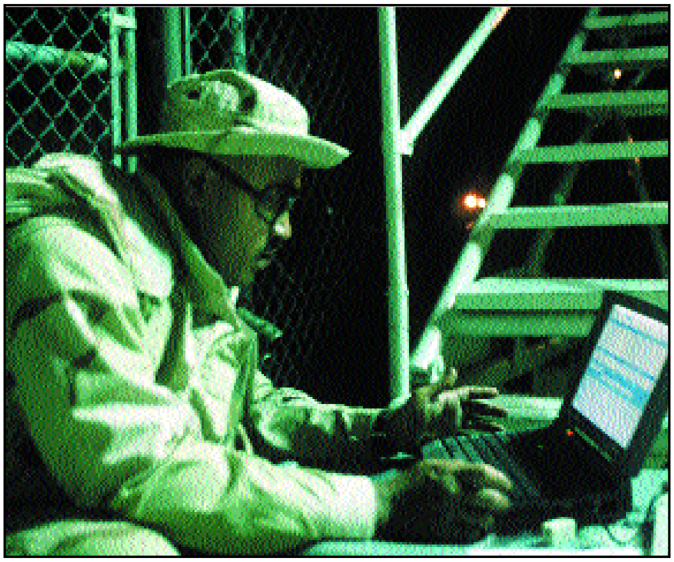
In FY 2000, AFIS initiated an organizationwide effort to accredit all AFIS systems within DITSCAP. A team from AFIS-HQ examined all field activities, conducted a security review, and gathered pertinent information. As FY 2000 closes, phase one of the DITSCAP process is well underway, with accreditation expected for all of AFIS in FY 2001.

Again in FY 2000, e-mail scripting worm attacks alerted AFIS to the need to combat the virus threat by coordinating action between AFIS-HQ and field activities. An AFIS-wide standard solution to the prevention, detection, and removal of viruses was developed, and AFIS is now working to incorporate the DoD Information Assurance Vulnerability Alert (IAVA) process. The plan has a staged response, allowing minor, single-computer virus incidents to be handled at the individual site while mobilizing forces AFIS-wide during a major attack.

AFIS developed prototypes and implemented several new technologies in FY 2000:

- Implementation of an intrusion detection system (IDS) at AFIS-HQ, with deployment to field activities planned for FY 2001
- Definition of a high-availability firewall architecture and deployment at AFIS-HQ, with deployment to field activities planned for FY 2001
- Initiation of a pilot program of routine vulnerability scanning, using a commercial tool
- Implementation of PKI/SSL on several AFIS web servers at AFIS-HQ and field activities
- Prototyping e-mail, server-based, virus-scanning software at AFIS-HQ, with deployment to all AFIS activities expected in FY 2001

AFIS also built IA into its internal development activities, addressing the three critical areas of enterprise architectural strategy, application development, and data access and availability. The enterprise architectural strategy is based on a multitiered platform (i.e., applications, data, and user interfaces are supported on separate platforms). The applications development strategy is based on thin-client interfaces for management and control of both the developed applications and COTS products deployed at AFIS. The data access and availability strategy is supported through the implementation of a straightforward backup and a plan for disaster recovery, as well as role-based access into the database for users and applications.



Using a laptop computer to track supplies.

The implementation of a multitiered platform ensures that information accessed and managed within the AFIS environment is safe and secure. The strategy calls for the implementation of four tiers: the client interface tier, the web server tier, the applications tier, and the database tier. The web server tier services all access to applications within the multitiered platform and interfaces with the applications tier for the access and management of applications. Built-in controls within the application server authenticate users and secure access to the applications. The application server also provides a single connection pool interface into the database, ensuring the integrity of stored and managed data. Only users and processes that have been defined within an application are able to access and manipulate data from the application server tier. The database tier is the single repository for data and is accessible by any user or application that properly authenticates to both the application server and the database.

The data access and availability strategy is supported through the implementation of a straightforward backup-and-recovery plan, as well as role-based access into the database for users and applications. The backup-and-recovery plan supports daily, incremental, and weekly backups of the database, ensuring the integrity of committed data.

DEFENSELINK AND BEST PRACTICES

AFIS manages DefenseLINK, the official DoD website. DefenseLINK runs on a sophisticated computer system that is operated by the Defense Technical Information Center (DTIC). Over the past year, DTIC has implemented a multitiered system design similar in function to that described earlier for the AFIS systems. DTIC is also completing the DITSCAP security review and has successfully passed several other major security reviews. DefenseLINK receives about one million page requests a week. It also gets about a dozen attacks daily from unauthorized intruders. Despite a high level of public availability and attempted attacks, DefenseLINK security has never been breached.

AFIS has gained valuable experience this year in maintaining a robust IA program. It has developed many beneficial practices that will serve it well in the future. Here are some of the lessons learned:

- Face-to-face site visits between AFIS-HQ personnel and field activities to initiate the DITSCAP accreditation process were invaluable in gaining full cooperation from all activities.
- AFIS-wide coordinated response to e-mail viruses is essential to eliminate duplication of effort and ensure fast response.
- Review of current security by independent experts quickly identified major vulnerabilities.
- Security management needs to be accomplished by personnel who can be dedicated full-time to the effort. Part-time security management by personnel with ongoing operational duties is ineffective.
- Effective security is a combination of (1) good system design, (2) continuous careful system monitoring, (3) immediate and effective response to intrusion detection, and (4) a well-trained staff.

DEPARTMENT OF DEFENSE INSPECTOR GENERAL

The Department of Defense, Office of the Inspector General (OIG) serves as an independent and objective official in DoD. OIG is responsible for conducting, supervising, monitoring, and initiating audits and investigations relating to the programs and operations of the DoD. In addition, the Inspector General provides leadership and coordination and recommends policies for activities designed to promote economy, efficiency, and effectiveness in the administration of these programs and operations, including the prevention and detection of fraud and abuse. The Inspector General is also responsible for keeping the Secretary of Defense and the Congress informed about problems and deficiencies relating to the administration of such programs and operations, the necessity for corrective action, and progress made.

AGGRESSIVE IA

In response to the Deputy Secretary of Defense's directives, the OIG has implemented an aggressive and proactive IA program. The program encompasses a multilayered strategy based on Defense in Depth (DiD) principles to defend against present and future threats to OIG information assets. The OIG IA program has made numerous improvements that will ensure continued success in terms of the availability, confidentiality, and integrity of OIG information and information systems. The goal of the OIG IA is to maintain a balanced, multilayered approach incorporating highly skilled IA professionals, well-designed and implemented IA policies and procedures, and the use of leading-edge technology in the defense of OIG automation resources.

Security police stand outside a missile alert facility perimeter.

In support of improving IA awareness among OIG personnel, the OIG conducted four separate awareness training sessions, using OIG technology resources. All new employees and contractors received security awareness training, and every member of OIG was required to attend this training. Also scheduled were various refresher training sessions. Security training is also made available on the OIG intranet.

Recognizing the fast pace of IA development, OIG responded by laying the foundation of future IA efforts by writing new policies and updating existing ones. For example, OIG updated its Internet policy to include user rights and responsibilities that had been absent in the original versions. Also updated were the Five-YearAutomated Information Resources Management Plan, the Microcomputer Antivirus Program Plan, and the Electronic Mail Policy. OIG conducted risk assessment of its Local Area Network (LAN) and implemented the Information Assurance Vulnerability Alert (IAVA) process, which ensured that the OIG systems administrators received, acknowledged, and complied with vulnerability alert notifications.

MAKING USE OF TECHNOLOGY

OIG substantially increased its IA stance through improving systems. The Office implemented an intrusion detection system (IDS), incorporated internal scanning procedures for electronic mail, and instituted scanning procedures for all incoming and outgoing Internet traffic. Related to that effort was the implementation of an automated incident response capability that captures and displays pertinent statistics on network activity and security information. These initiatives ensured the availability and integrity of critical OIG computing assets. OIG has also continued to improve and update its firewall by evaluating new products and services.

In support of DoD PKI efforts, OIG began to implement its PKI program by procuring initial hardware and software. OIG also identified management personnel needed to support implementation of the PKI project and projected resources needed over a five-year period to deploy PKI at OIG HQ and at local field offices.

In an effort to ensure the availability of OIG information assets, the OIG's IA program during fiscal year 2000 has continued to add more protective measures. Besides the enhanced intrusion detection capability, OIG has continued to place increased interest in security awareness training and invested in new technology designed to protect vital information and provide first-class computing assets to OIG personnel. OIG will continue to implement innovative and aggressive methodologies to ensure the protection of its information assets. The OIG IA program will also continue to implement projected DoD IA initiatives such as PKI and to act as an integral partner supporting the overall DoD plan to protect the nation's vital information resources from compromise.

OFFICE OF THE UNDER SECRETARY OF DEFENSE (ACQUISITION , TECHNOLOGY AND LOGISTICS)

For many years now, the DoD has been at the forefront of IA and Critical Infrastructure Protection (CIP) R&D. Information and communications are at the core of every military activity and critical to the mission of the DoD, which is to provide the military forces necessary to protect the security of the United States. As such, IA and CIP R&D play a crucial role in the DoD's goal toward achieving Full Spectrum Dominance, as outlined in Joint Vision 2020. The overall R&D program includes five primary thrusts in the areas of Information Assurance, Threat/Vulnerability/Risk Assessments, System Protection, Intrusion Monitoring and Response, and Recovery and Reconstitution.

The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics [OUSD(AT&L)] is responsible for all DoD science and technology (S&T) strategic planning, budget allocation, and program execution and evaluation. One of the primary responsibilities of the OUSD(AT&L) is to coordinate the portfolio of DoD S&T programs to meet the needs of both the Department and the National Defense S&T objectives. In a similar fashion, the OUSD(AT&L) is involved in the coordination and collaboration of international S&T programs with member-states of the North Atlantic Treaty Organization (NATO), as well as other recognized allies within the international S&T community.

The Information Systems Technology (IST) Reliance Panel reports to the Deputy Under Secretary of Defense for Science and Technology [DUSD(S&T)] within OUSD(AT&L). The IA subpanel is one of five subpanels of the IST Reliance Panel and is responsible for coordinating the DoD efforts in IA S&T research. DARPA and the Services' S&T investments for IA were reviewed in FY

Military personnel push supplies onto a C-130 Hercules aircraft.

2000 through the IST Technology Area Review and Assessment (TARA). The high-quality, focused S&T programs described below received strong endorsements from the TARA subpanel and were highly relevant to the national interests regarding IA.

IA Retention

In an effort to increase the amount of scientific talent and research being applied to national concerns regarding IA, the ODUSD(S&T) has sponsored two separate Broad Agency Announcements (BAAs) detailing new University Research Initiatives (URIs) in the areas of Critical Infrastructure Protection (CIP) and IA. The first BAA, announced in June 2000, established a Critical Infrastructure Protection and High-Confidence, Adaptable Software (SW) URI Research Program. This BAA was intended to provide an individual award for up to five years for research within any of 13 topics identified as critical to IA. The second BAA, also announced in June 2000, established a CIP and IA Science and Engineering Augmentation Award for Fellows. The Fellows Award was designed to provide opportunities for scientists and researchers in fields such as physics, mathematics, computer science, and engineering to learn and conduct research in the areas of CIP and IA. The program was structured as a mentoring program that teams the Fellows with DoD-awarded principal investigators already conducting research in the area of IA. The mentor program was intended to accelerate the integration of scientific talent and establish it within CIP and IA, foster interactions for future collaborations, and help universities expand the CIP/IA research community.

IA Accomplishments

The following accomplishments are highlights of Science and Technology efforts by DARPA, the Service laboratories, and research offices within the purview and strategic oversight of the IST IA subpanel. These programs are jointly reviewed and coordinated to ensure that the scope and depth of the programs meet DoD needs.

In a joint venture, the Air Force Research Laboratory (AFRL), located at Griffiss Technology Park in Rome, New York, and Cornell University have established the Information Assurance Institute. This unique initiative was developed to focus on issues pertaining to the proliferation of mobile code, with future efforts planned in the areas of fault tolerance, reliable cybersystems, and the use of data mining in intrusion detection.

Two separate efforts in IA related to command-and-control (C2) protection: The first was the development and porting of a COTS Intrusion Detection System for applications within the Force Battle Command Brigade and Below platform. This initiative incorporated commercial authentication technology used to seal standard message formats. The C2 IA initiative also resulted in the establishment of a

Tactical Internet (TI) security baseline through vulnerability assessment, analysis, and testing. This TI was then used as a platform for testing second-generation security measures with Intrusion Detection Systems and other available security tools. This effort also resulted in the development of a suite of red team attack evaluation tools and a Security Manager Graphical User Interface for overall network status management, monitoring, and visualization.

The second C2 initiative was the development of the Cyber Command System (CCS). While the capability demonstrations to date have shown the CCS to still be in its infancy, the technology offers potential for the future of C2 operations. CCS was initially intended to provide C2, course of action, and an incident response framework for hierarchical data networks. Once fully proven, CCS has the potential to support cybersituation understanding, visualization, and policy management, as well as automatic and human-assisted dynamic incident response.

Several technologies are under way for the use of situational awareness across the information and digital landscape. The Network Fuzzy Logic Attack Recognition Engine (NET-FLARE) was developed to assist the information warriors in the missions and situations that they support by filtering large amounts of raw Information Warfare (IW) data into usable formats. This effort is intended to improve the use of available data needed for making critical decisions and to reduce the cognitive dissonance associated with incorporating overwhelming amounts of information. NET-FLARE also provided a way of visualizing the current IW state and allowed for the dynamic creation of mission-based IW decision policies.

The Distributed Agent Information Warfare Framework was another initiative intended for monitoring and visualizing activity across the network landscape. This system was designed to incorporate system agents across the network for the identification of system activities ranging from host- to traffic-level events. Host-level events are collected through the use of dynamically distributed field agents used to detect coordinated distributed attacks.

Through the efforts of DARPA, OUSD(AT&L) has addressed several issues pertaining to the field of IA experimentation: First of all, it has succeeded in raising the level of awareness and effort being applied to critical and challenging technical problems not currently being addressed by either industry or other government programs. Next, it has established a set of requirements to support the use and development of high-quality, science-based, hypothesis-driven experimentation. DARPA has also built, and now operates, a networked computer laboratory facility, including virtual private networks, intended to encourage remote collaboration on projects related to IA experimentation.

In addition, DARPA has promoted the area of IA scientific red teaming by engaging the red team as a partner in the experimentation and learning process. This effort has created a means of identifying major differences between attacker and defender strategies. It has also identified opportunities for thwarting the intelligence preparation, planning, and execution of malicious activities by potential adversaries. The concept of whiteboarding was also developed as an efficient, cost-effective means of interrogating the strengths and weaknesses of potential attack-defend scenarios. This technique was particularly useful in providing direction in the early steps of experimentation by identifying disagreement with regard to potential attacker-defender scenarios and by indicating possible future directions in experimentation.

Making Use of IA Technologies

The DoD IA S&T community has developed several critical technologies associated with improving intrusion detection. The Automated Intrusion Detection Environment (AIDE) Advanced Concept Technology Demonstration (ACTD) successfully demonstrated a three-tier reporting structure that included multiple Services and CINCs at 12 different locations. This capability enabled the detection of low-level coordinated attacks that would have been otherwise unobservable by incorporating correlated automated event filtering, reporting, and visualization techniques.

The Extensible Prototype for Information Command-and-Control (EPIC2) Architecture is another example of progress made in the area of intrusion detection. Experiments have demonstrated the successful exchange of IA event data between Australian Shapes-Vector and the EPIC2 prototype intrusion detection systems. Under the Air Force Enterprise Defense program, EPIC2 provided enhanced change management and intrusion detection capabilities to the Air Combat Command Network Operations and Security Center.

The program EMERALD demonstrated the development of a complete intrusion detection architecture and sensor system and has been shown to significantly outperform similar COTS intrusion detection systems. It has been deployed to operational sites for experimentation in locations such as the Joint Intelligence Center, Pacific in Hawaii.

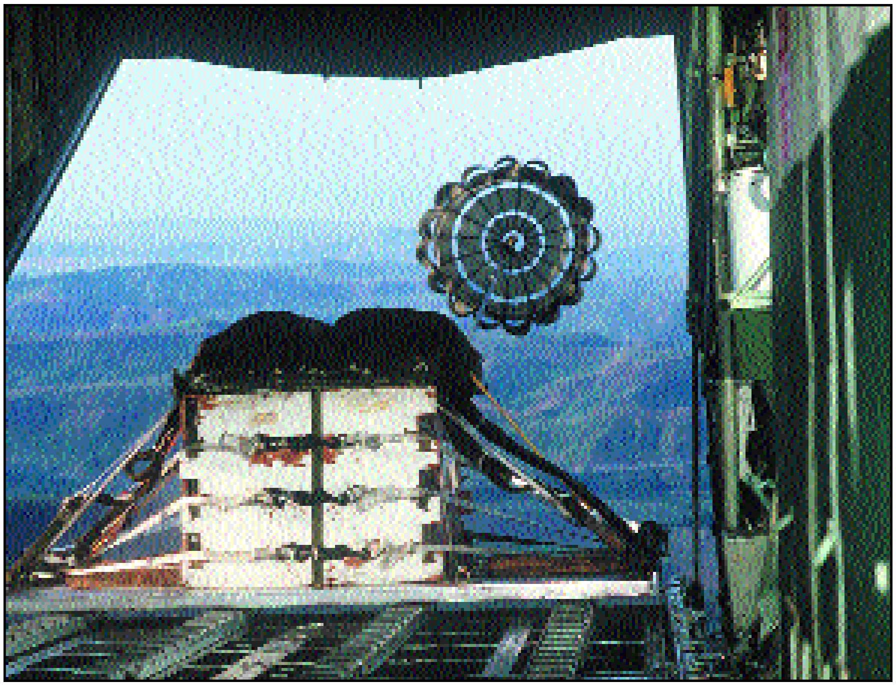
The Intrusion Detection and Isolation Protocol was also developed to provide an architecture and components for managing intrusion detection and response. It was initially intended as a way to rapidly prove concepts related to intrusion detection and has evolved into an integrated system with significant potential.

Finally, a program named DYNAT was created, intended as a TCP/IP spread spectrum technique for application in closed community networks. Based on the principle of dynamically switching IP addresses for community members, it has dramatically improved the ability to detect network intrusions.

OUSD(AT&L) fostered the transition of the Naval Research Laboratory Requirements Analyzer Toolset to members of industry, government, and academic institutions. This toolset discovered critical flaws in contractor-produced specifications for Navy Submarine Torpedo Tube Control Panels. The toolset has also been incorporated into the software engineering courses at Stanford, University of Oregon, University of California-Irvine, and the University of Utah.

The Cryptographic Protocol Analysis Tool was developed by the Naval Research Laboratory. It was used to analyze industrial protocols for the Cellular Telecommunications Industry Association and helped identify flaws in several existing protocols such as the Internet Key Exchange Protocol. The tool was also used to specify the requirements for the Secure Electronic Transitions Protocol.

The DoD S&T Community has also been instrumental in the development of needed software operating system (OS) wrappers used for enhancing system security. New OS wrappers were developed for many of the COTS operating systems in existence today and offer significant new capabilities in host protection. The wrappers were intended to provide elements of trusted path and control (e.g., between a keyboard and a smart card), safe execution environments, and protection against writing to removable media.



Supplies are dropped from a cargo plane.

DEPARTMENT OF DEFENSE EDUCATION ACTIVITY

The Department of Defense Education Activity (DoDEA) directs operations and planning for the worldwide DoD network of 220 schools and 112,000 students, consisting mostly of military dependents. In total, it has a presence in 14 foreign countries, seven states, Guam, and Puerto Rico.

The DoDEA IA initiatives combine products and services from the private and public sectors in a balanced approach to the protection of DoDEA information assets. DoDEA has been active in developing policy and programs to establish IA guidance for its activities. IA awareness training programs were drafted for senior executive, systems administrator, and user target audiences. The IA awareness program is being implemented in DoDEA HQ, and compliance down to the school level is targeted by October 2001. DoDEA also developed a Security Test Plan and Procedures Report to document the process for verifying the integrity of in-place security features of the DoDEA HQ network for their sufficiency to protect the network.

From an operational perspective, DoDEA initiated the certification and accreditation (C&A) process for the DoDEA HQ network in accordance with DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP, November 1977). A risk analysis of DoDEA HQ assets, threats, and vulnerabilities was conducted to identify the risks associated with processing information on the DoDEA HQ network.

DoDEA also took an active technological approach by installing commercially available firewalls at the perimeter of the DoDEA HQ network, monitoring network activity through these firewalls, and maintaining the firewalls by ensuring that newly discovered vulnerabilities are addressed quickly. In addition, DoDEA installed antivirus software at both the server and workstation levels. It ensures the currency of the antivirus software by automatically downloading and installing the latest versions of antivirus software and any required patches on a regular basis to the servers and to each and every workstation at the workstation level.

DoDEA heightened information assurance awareness, elevated security as a primary objective in its information technology program, and significantly reduced its vulnerabilities. DoDEA’s goal is to achieve a seamless IA environment from Headquarters to the schools across the full spectrum of operations.

MILITARY HEALTH SYSTEM

The mission of the Military Health System (MHS) is to support the Department of Defense and the nation's security by providing health support for a full range of military deployments and to sustain the health of members of the Armed Forces, their families, and other individuals who qualify. The MHS's IA standing goals are to protect the readiness information of the warfighters and to protect the privacy of beneficiaries. The MHS develops tri-Service systems that require interaction among Services and commercial and Federal partners. This environment creates unique security considerations that the MHS addresses proactively in its daily operations.

During the next year, the central focus for MHS IA initiatives will be the implementation of the Health Insurance Portability and Accountability Act (HIPAA), which requires standardized transaction sets, security controls, and privacy of electronic health-related information. Application of HIPAA throughout MHS will ensure the utmost level of protection of sensitive data and will support MHS's commitment to the privacy of the beneficiary.

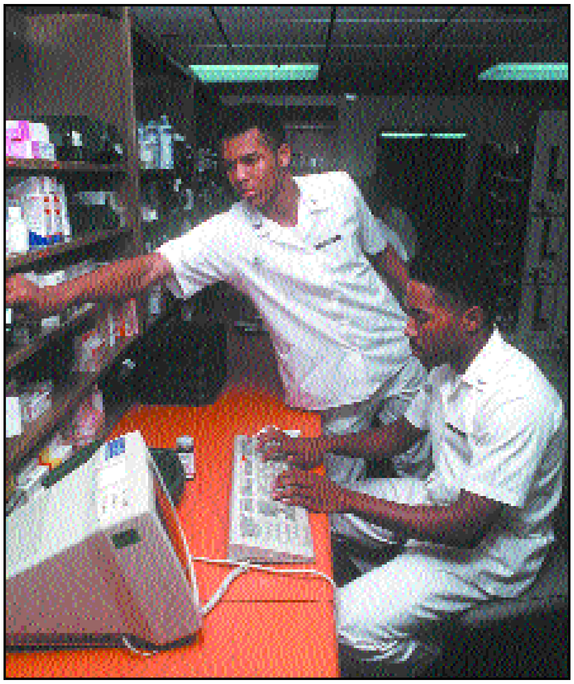
IA INITIATIVES

MHS has aggressively implemented many key IA initiatives in FY 2000 and has many others actively in progress to significantly enhance the DoD medical community's IA posture. MHS has aligned ongoing IA initiatives with the "DoD Information Assurance Through Defense in Depth" approach to ensure that its people, operations, and technologies support the multidimensional layers of effective security protection.

MHS has a dedicated IA staff comprising security professionals whose experience, capabilities, and credentials map to a cross-section of IA functional areas. The number of IA support personnel at the Program Office level has been increased from 20 to 31 to expand MHS IA core capabilities and ensure timely and effective responses to a wide variety of IA actions in support of MHS customers. The MHS has identified key roles required to support its IA program: Chief Information Officer (CIO)/Designated Approving Authority, IA Program Manager, Information Systems Security Manager, Information Systems Security Officer, Systems Administrator, Network Administrator, and Application Program Managers.

MHS personnel have completed comprehensive training on varied IA topics during FY 2000 to increase IA core competencies, including these three examples:

- Registration Authority and Local Registration Authority training to support PKI initiatives
- National Defense University Certification Courses for Information Systems Security Professionals (compliant with NSTISSI 4011)



Two pharmacy technicians use the Composite Health Care System, a network that links various medical and administrative functions.

- NSA's Information Security (INFOSEC) Assessment Methodology (IAM) course

In addition, MHS developed an initial version of automated online tools for all users at the workstation to enforce DoD security training requirements. An automated message on the tracking database for required training directs the user to complete training before initial logon and for subsequent annual refresher training. The online training covered IA policy, secure computing, Internet/electronic mail, media management, threats and vulnerabilities, risk, incident reporting, certification, and protection of patient information. MHS also developed an initial version of automated online training tools for technical network users such as engineers, systems administrators, and technical developers.

MHS expanded its IA website to provide online requests for accreditation reports, accreditation process templates, and guidelines and examples. Also created were an MHS Computer Emergency Response Team (CERT) link, virus resources, and vulnerability alerts. In order to expand MHS policy awareness, links were added to MHS's automated information system (AIS) security policy, legislative reference guides, and frequently asked security questions, with the capability to send queries directly to the MHS Security Team. MHS filled a position on the DoD Health Insurance Portability and Accountability Act (HIPAA) Integrated Process Team to provide expertise in the development of an HIPAA training program for all government agencies that handle or transmit patient information.

MHS IA personnel created MHS IA policies to identify and track security requirements and responsibilities as they apply within MHS. They revised existing MHS AIS policy to reflect current DoD and MHS security requirements and formulated upgraded MHS IA policy to meet the challenges of new initiatives such as PKI and HIPAA. They also drafted (1) an MHS

PKI Policy and Implementation Guide to ensure a standard implementation of the DoD PKI within the MHS and (2) a policy to document DoD Information Assurance Vulnerability Alert (IAVA) notification processes within MHS.

MHS developed standard operating procedures (SOPs) to certify and accredit MHS systems, as well as procedures to document DoD and DISA IAVA notification processes within MHS. These C&A procedures included a comprehensive checklist of all Federal and DoD certification requirements (including the Clinger-Cohen Act requirements) and were developed and made available to MHS clinical AIS project managers. The use of these procedures will ensure compliance with all applicable requirements, while also ensuring standardization across the MHS. Management of the C&A process was further enhanced through the development and implementation of an automated database tool that will enable selective data gathering, data analysis, emphasis-area tracking, and improved reporting. MHS systems undergo a formal certification process based on the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) methodology and the Common Criteria Controlled Access Protection Profile to meet applicable requirements. MHS conducted Certification and Accreditation of medical information systems and accredited 7 MHS systems and provided 10 Interim Approvals to Operate (IATOs). Currently, there are 26 systems/applications in different stages of the C&A cycle.

IA Program

MHS maintains many other ongoing IA operations programs, including incident response, certification and accreditation of systems, and assessment of the MHS IA program. Under incident response, MHS maintains an enterprisewide IAVA tracking-and-reporting capability with its Military Health System Computer Emergency Response Team (MHS CERT). This program ensures that advisories and patches are implemented and reported back to DoD and the three Services. MHS developed MHS CERT process improvements for timely response tracking and for upstream reporting purposes. These improvements include more comprehensive and timely dissemination of alerts to the Services and to the Program Managers, involvement of the Program Managers in enforcing the implementation of patches, and use of automated methods for posting suspense dates and for follow-up action tracking.

To assess the effectiveness of the current MHS IA program, the IA staff follows a process based on NSA’s INFOSEC Assessment Methodology (IAM). The assessment validates compliance with DoD security requirements and standards and HIPAA. In addition, research, review, and analysis of commercial health care requirements and prospective security countermeasures are performed to assess the impact of MHS and partner implementation. MHS also provided service by initiating a streamlined process for the Services to obtain "Networthiness Certification" of hardware and software for systems.

MHS pursued proactive efforts in daily IA operations to defend its computing enclave. It assigned usernames, passwords, PINs, user accounts, and privileges in the routine employment of Health Affairs/Office Automation (HA/OA) network operations. It used management tools to perform file encryption, network monitoring, and vulnerability checking.

IA Technologies

In defense of its enclave boundary, MHS centered efforts on developing firewall technology. It developed and started implementing a standard MHS security firewall solution for hospitals and clinics located on Service bases, posts, camps, and stations. In partnership with Navy Space and Warfare Command (SPAWAR), it developed a standard configuration of firewalls located on Navy installations. MHS worked with the Air Force Communications Agency (AFCA) and Langley AFB to test a standardized firewall solution to protect all medical traffic going through AFB enclaves. The AFCA is developing a standard implementation practice for bringing all Air Force hospitals and clinics behind the protection of the AF Barrier Reef Program. Finally, scanning MHS automated information systems allowed MHS to conduct vulnerability assessments in support of the certification and accreditation process.

In defense of its networks, MHS developed Defense in Depth (DiD) technologies and tools for a Virtual Private Network (VPN) and an Intrusion Detection System (IDS) suite of equipment for Army and Navy sites. At Langley AFB, MHS worked with the AFCA to test the standard Air Force intrusion detection solution. The AFCA is developing a standard implementation practice for all Air Force bases that will integrate hospitals and clinics worldwide. The MHS is supplying the VPN devices for all Air Force hospital sites. The MHS standard VPN solution was implemented at the Defense Enterprise Computing Center in Montgomery, Alabama.

In ongoing PKI efforts, MHS set up PKI Local Registration Authority workstations for the implementation of DoD-directed PKI. On this same front, a PKI implementation strategy team was established to support the managed care support contractors using Interim External Certification Authorities (IECAs). MHS took an active role in the development of PKI policy by forming a PKI team to develop the security architecture necessary to comply with DoD PKI network implementation requirements. This team included MHS business partners whose systems must be interoperable with the DoD

PKI program. The team identified functional roles and responsibilities within MHS for PKI implementation. Major business partners include Department of Veterans Affairs, Veterans Health Administration, Indian Health Service, National Institutes of Health, and 12 major managed care support contractors. MHS maintained a significant presence in DoD PKI working groups through PKI briefings and facilitation of interoperability dialogue among organizations. Internally, a prioritized list of MHS systems and timelines for Public Key Enabling (PKE) was developed.

To support DIAP's IA Readiness Assessment workshop, MHS assisted in the development of metrics for the DoD to assess how well Services and Agencies are implementing IA initiatives. The MHS IA Working Group hosted consolidated discussion forums to capture the following security-related issues: applying DoD and MHS security policies within MHS, to its sharing partners, and for its beneficiaries; employing protection technologies such as PKI and encryption throughout MHS; and meeting site-level requirements throughout the Services for MHS AIS deployments. Finally, MHS upgraded the tracking system for the ADP "clearance" application process, replacing hard copy forms with electronic tools and thus significantly decreasing the vulnerabilities associated with handling and processing sensitive personal data (e.g., Privacy Act) in hard copy format.

Throughout FY 2000, the MHS IA staff has firmly focused on enhancing its already successful IA program. Efforts were directly responsive to the MHS IA goals of protecting its readiness information and privacy and to correspond to Defense in Depth strategies. MHS will continue to apply best practices and technical solutions to ensure within its organization the highest level of IA, commensurate with current industry standards.

UNDER SECRETARY OF DEFENSE (PERSONNEL AND READINESS)

The Office of the Under Secretary of Defense (Personnel and Readiness) [OUSD(P&R)] reevaluated its IA posture and made a number of changes designed to better support the mission of the program. The first change was to merge the IA program with the Critical Infrastructure Program (CIP), which will eliminate redundant activities and allow the project staff to work on both the infrastructure and the security aspects of systems and resources.

A combined IA/CIP plan has been drafted and is currently under management review. This plan should allow better execution of the project while reducing overall resources expended. In addition, it will provide for a more coordinated and less burdensome approach to communicating with the systems and resource owners and with the operators at both the Service Headquarters and in the field.

Given preliminary general management approval of the direction of the IA/CIP plan, the OUSD(P&R) staff has begun executing the first step: system and resource identification. This identification is both for mission-critical systems needed for CIP and for systems that have some level of vulnerability requiring IA support. To bring in contractor staff to assist in the execution of the plan, a statement of work is also being developed.

Members of the 82nd Airborne Division parachute a from a C-141 Starlifter aircraft.

To specifically address issues and coordinate information among the entire Personnel Community, OUSD(P&R) has established a working group with its Service Personnel counterparts. This is a very difficult task because IA and CIP are not ordinarily handled within the Service Personnel Community's area of responsibility. The establishment of this working group is driving the development of linkages among each of the Services' Personnel, Security, and Information Technology organizations.

WASHINGTON HEADQUARTERS SERVICES

Washington Headquarters Services (WHS), located in the Pentagon, is the DoD Field Activity that provides a broad variety of operational and support services to the Office of the Secretary of Defense (OSD), specified DoD Components, selected other Federal Government activities, and the general public. Areas of support include financial management and accounting services, directives and records management, civilian and military human resource management, personnel security services, information technology and data systems support, facilities management, office services, physical and information security services, law enforcement and protection, voting assistance and legal services.

Defense in Depth Strategies and Implementation

In 1998, WHS developed a program entitled "Information Assurance Awareness Training" and has been operating it successfully ever since. It has implemented a computer-based training (CBT) and testing user-certification program that covers topics such as passwords, incident reporting, roles, responsibilities—general as well as personal—and security practices. Once users are certified, they are granted access to the WHS network and assigned enclave. This has created a security-aware cadre of users that performed exceptionally well during the significant virus attacks this year.

WHS uses a Defense in Depth (DiD) strategy to guard against viruses. This strategy begins with intrusion detection and antivirus software on the mail transfer agent, mail servers, and workstations. Rapid detection and rapid technical response to new and unknown viruses have proven highly effective. However, the best protection against virus attacks is a workforce that is aware of security issues and that knows when not to open potentially virus-laden e-mail, documents, spreadsheets, or other attachments of unknown origin. Signature updates are done routinely for WHS workstations. WHS personnel apply a "delete if suspicious" policy that states that a user must delete any mail or attachment that has been received when the recipient does not know the sender or is not expecting a specific type of message or attachment.

WHS implemented Security Technical Implementation Guidelines (STIGs) on its workstations and servers in the UNIX and NT environments and is awaiting the DISA guidance on NetWare that is running in one of its enclaves. WHS has taken the additional step of developing and implementing a Waiver Process and Preprocessing Guide for each of the WHS Components. Business processes may not always work as intended when the STIGs are rigorously applied. Extensive diagnosis and analysis are needed once the offending STIG is isolated. Depending on the assessed risk involved, a waiver is then developed in accordance with the Guide and reported to DISA.

In connection with the STIGs, WHS is funding DISA to perform Security Readiness Reviews (SRRs) on a regular basis. These reviews have improved the WHS security posture and have raised the security awareness of WHS Directors, IT Managers, and users. Over the past two years, these SRRs have documented steady improvement in the WHS security posture. The outcome is that WHS has evolved to a point where security awareness is a part of the culture.

The September 2000 SRR of WHS by DISA indicated that the implementation of the STIGs in WHS is the best one that it has seen so far. WHS also participates in the DISA-sponsored annual Technical Interchange Meetings on the evolving STIGs. A derived benefit from this activity is that it provides vulnerability assessments of the infrastructure, produces the Security Test and Evaluation (ST&E) portion of the DITSCAP, and accounts for more than half of the work required in developing a System Security Authorization Agreement (SSAA).

The WHS Components have achieved Certification and Accreditation (C&A) of their Automated Information Systems Security Plan (AISSP) from the Designated Accreditation Authority (DAA). WHS, however, sent a draft Administrative Instruction (AI) out for review that changes this process to the one required by DoD Instruction 5200.40, "DoD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)," December 1997. Upon approval, the AI will require WHS Components to use the DITSCAP to certify and accredit all new WHS Component information systems, as well as those requiring recertification. The new process is much more encompassing than the system that it replaces, with associated resource implications for WHS.

Working inside an AN-TSC93B Tactical Satellite Terminal to communicate with forward units in Bosnia.

For more than a year, WHS has been implementing the IAVA program with the assistance of DISA. WHS has made already significant strides on the IAVA implementation: It has registered the CIO, the WHS Network Manager, and the WHS Information System Security Manager (ISSM) into the Vulnerability Compliance Tracking System (VCTS) run by DISA. During the first quarter of CY 2000, network assets were entered into the VCTS. By April 2000, WHS had also registered all the IT Managers, ISSMs, Project Managers, and Systems Administrators into the IAVA program. As they were registered in the VCTS, the Systems Administrators began registering assets, and by early 2000, WHS was acknowledging IAVA and reporting compliance through the VCTS.

A tower operator on the sunrise shift.

Deputy Secretary of Defense DoD PKI memorandum of 6 May 1999 and the update by the DoD CIO of 12 August 2000 define DoD policies for the development and implementation of a Departmentwide PKI and establish very aggressive milestones. WHS provides PKI Registration Authority (RA) and Local Registration Authority (LRA) services to both the WHS and OSD staffs. Initial efforts have been directed at identifying and issuing certificates to the OSD and WHS private web servers. Eighteen servers have been identified, and 15 have received their certificates. At the same time, a survey of the WHS staff determined that approximately 1,500 WHS personnel will require PKI certificates. Each WHS Directorate will require an organizational LRA to issue replacement certificates and perform encryption key recovery tasks. An LRA workstation, printer, smart card reader, and smart cards have been purchased for each Directorate.

A small on-site contractor support initiative developed a WHS PKI implementation plan. Upon completion of the plan, both contractors will be issued LRA credentials and will start issuing the initial PKI identity certificates, e-mail signing certificates, and e-mail encryption keys to all WHS employees.

All edge routers and switches under WHS Network Management control have been located, recorded, and maintained in a configuration control environment. In addition, VCTS assists with device tracking, software configuration, and vulnerability alert implementations. Troubleshooting and problem solving have become much easier with the implementation and management of a single network under rigorous configuration control to support WHS.

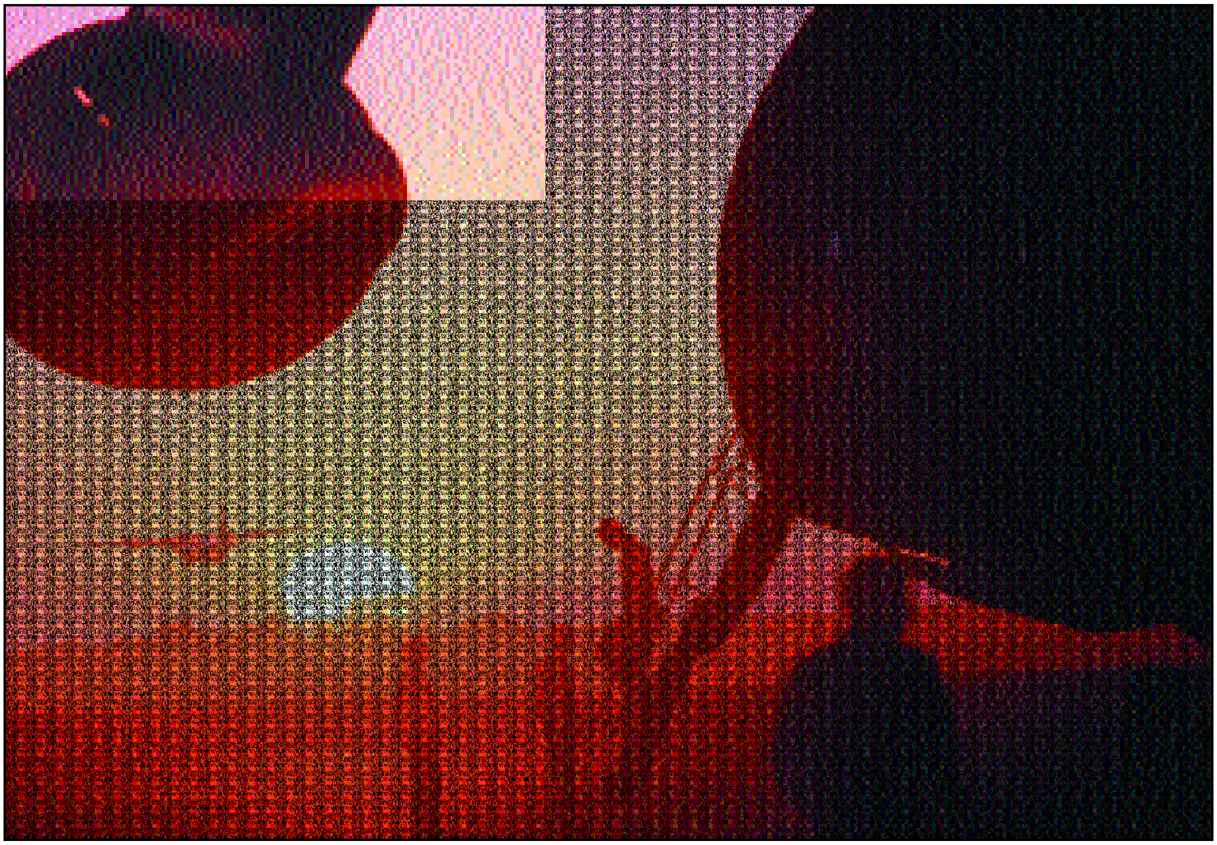
WHS has implemented a well-defined and controlled perimeter to protect the networks that it is responsible for: First, WHS has deployed a strong set of access control list rules at the nexus of the WHS network, followed by a robust intrusion detection system. Second, a WHS firewall, with a much stronger access control list than the one that NISA-P uses for the overall Pentagon, guards against unauthorized access to the WHS enclave domains. Third, one enclave with very sensitive personnel information has a firewall running inside the WHS firewall, behind the enclave edge device. Fourth and most important, NISA-P is running Pentagonwide access control lists, intrusion detection, and firewalls.

To filter incoming and outgoing traffic, the WHS Network Manager has implemented Access Control Lists (ACLs) on the routers. These ACLs help to prevent unauthorized access into or from the networks connected to these routers at the ingress or egress points of the WHS network. The configuration and ACLs are stored in the WHS backbone server and are maintained on the basis of inputs from the intrusion detection system, vulnerability alerts from DISA or NISA-P, and the WHS IT Managers. ACLs are reviewed against the off-line standard to ensure that no unauthorized entries were added.

Making Use of Technology

The firewall requirements associated with the WHS enterprise were determined and analyzed with the help of the WHS Network Manager, NISA-P, and DISA. An approved firewall protection product, which is now in the process of being installed and tested, has been procured. As in the configuration and ACLs for WHS router filter access control, rule sets for the WHS firewall are developed, based on inputs from the intrusion detection system, vulnerability alerts from DISA or NISA-P, and the WHS IT managers. Firewall system monitoring and maintenance includes the verification of hardware and software operation. The integrity of the system must be constantly guarded to prevent unauthorized access to the systems behind the firewall. The firewall server is routinely checked to ensure operational status and that unauthorized personnel have not altered the rules for the system.

The Intrusion Detection System (IDS) monitors system logs and checks them for unauthorized access or attempted unauthorized access. Real-time monitoring of



A C-130 Hercules aircraft takes off as a section of a C-5B galaxy is silhouetted in the sun.

network traffic detects both external and internal threats and includes port scans, IP addresses range scans, and other types of activity capable of detecting a potential threat before it becomes an exploited vulnerability. The IDS provides real-time information that alerts network management personnel to take immediate (or watchful) action on apparent threats against the system. Suspected external intruders are immediately blocked at the router or WHS firewall and subsequently reported to the network management personnel and designated WHS security personnel. Depending on the nature of the threat, the intrusion may be reported to NISA-P as well. Suspected internal intruders will be identified and immediately reported to network management personnel, designated security personnel, and appropriate leadership, as well as IT and security personnel in the affected WHS Component.

An upgrade to the WHS network is currently in process, with the establishment of a new FDDI ring that will physically (as opposed to logically) place all WHS Components behind the main WHS routers. Upon its completion, the network will be recertified under the DITSCAP process.

Under a DoD Directive entitled "Single Agency Manager (SAM) for Pentagon Information Technology Services," NISA-P manages the Pentagon backbone network for Pentagon tenants. This management responsibility includes the architecture up to the enclaves, with their subnetwork components. More specifically, NISA-P manages the Pentagon legacy backbones, the newly renovated space backbones, and an early backbone that will replace the legacy backbones that lack performance, security, and configuration management. All circuits from locations external to the Pentagon have been located, documented, and are tracked in a configuration management environment. Legacy circuits internal to the Pentagon are also tracked; however, the circuits in the renovated space are managed and controlled by NISA-P, with WHS maintaining the configuration history of these legacy circuits to assist NISA-P in troubleshooting and problem solving.

For WHS, NISA-P manages the backbone from the two main Pentagon routers to the two WHS routers at the edge of the WHS network and the WHS OU2-level mail server. NISA-P also performs Pentagon-level intrusion detection, monitoring, firewall management, and access-control filtering. If an intruder makes it through those control gates, it is then up to WHS to provide the final layer of Defense in Depth, which it is doing very well.

The WHS Information Technology Management Board (ITMB), comprising representatives from each Component, serves as a consensus-based management board that centralizes WHS IT planning and management and ensures that WHS Component interests are represented in the WHS IT program. The ITMB also ensures that WHS Components adhere to applicable IT standards, maintain a WHS common architecture, maintain a WHS standard secure operating environment, work toward centralizing common support areas where appropriate, review planned initiatives across WHS, and participate in the development of fair and equitable resource allocations for WHS IT.

WHS has forged a partnership with the Field Security Operations (FSO) Office of the Defense Information Systems Agency (DISA) to assist in the design and management of our security architecture and to provide independent Security Readiness Reviews (SRRs) to validate the integrity of our Defense in Depth strategy. With DISA's assistance, WHS has installed the National Security Agency/DISA-approved registry and file access control lists on its servers and workstations and is working with DISA to obtain the same level of protection for its other COTS networks.

With the establishment of a centralized Network Management Team and an IAVA Security Team, WHS has implemented a broad spectrum of network services, including audit, access-control list router management, intrusion detection, and operational network monitoring and control, into the DoD SMI. Extensive familiarity with the security aspects of a DoD-wide GIG is enhanced through WHS's teaming effort with the DISA Field Security Operations and participation in the IAVA program. WHS's abilities to identify unauthorized access either to the network or to information and to identify specific users of the network are important factors in dealing with the insider threat.

In conclusion, over the past year and a half, WHS has significantly improved its security posture by implementing a new enterprise network that was designed, with assistance from DISA, with security foremost, including firewalls and intrusion detection. Implementing the DISA STIGs across the enterprise and installing the DISA IAVA/VCTS system have also strengthened operational security. Most important, WHS has achieved significant improvements in security by training and indoctrinating its personnel on proper security procedures, which has resulted in the ability of the enterprise to continue operations during the significant virus attacks on the e-mail systems over the past year.

JOINT CHIEFS OF STAFF

The U.S. Military has nine Unified Commands. The term "Unified" refers to the multi-Service or "joint" nature of these Commands from all branches of the Armed Services, "unified" by one Commander in Chief (CINC) charged with car rying out the Command's mission. Each of the nine CINCs is either a four-star Army, Marine, or Air Force general or a Navy admiral.

Five CINCs have a Geographic Area of Responsibility (AOR):

- U.S. Joint Forces Command (USJFCOM), headquartered in Virginia
- U.S. Pacific Command (USPACOM), headquartered in Hawaii
- U.S. European Command (USEUCOM), headquartered in Germany
- U.S. Central Command (USCENTCOM), headquartered in Florida
- U.S. Southern Command (USSOUTHCOM), headquartered in Florida

Each of these CINCs is responsible for conducting all military operations within its assigned geographic region. For example, military operations in the Persian Gulf region, such as the recent Operation Desert Thunder, are the responsibility of the CINC, U.S. Central Command, because that region is part of his assigned geographic area of responsibility. USJFCOM's geographic area of responsibility consists mostly of the Atlantic Ocean.

CINCs with Geographic Areas of Responsibility are the highest-ranking military officers in the chain of command for the conduct of military operations. They report directly to the National Command Authorities, which consist of the Secretary of Defense and the President of the United States.

The four other Unified Commands have responsibilities that are functional, not geographic, in nature:

- U.S. Transportation Command (USTRANSCOM), headquartered in Illinois
- U.S. Space Command (USSPACECOM), headquartered in Colorado
- U.S. Strategic Command (USSTRATCOM), headquartered in Nebraska
- U.S. Special Operations Command (USSOCOM), headquartered in Florida

For example, U.S. Transportation Command is responsible for the large-scale movement of military equipment, supplies, and personnel throughout the world, using logistics aircraft and ships.

The Joint Service aspect of each of the Unified Commands provides a vital link in coordinating all the Services in a particular AOR or mission area. In performing their mission, the Unified Commands draw upon each Service's strength. This efficient integration of U.S. military forces into one potent and streamlined force is the overall goal of Joint Vision 2020.

Significant progress has been made in the area of Defense in Depth (DiD) implementation this year. The DiD implementation strategy is divided into three phases: (1) publish a DiD brochure that provides a general overview of the DiD approach, (2) revise Joint Staff policy on DiD, and (3) publish new Joint Staff policy to provide the "how-to" guidance to achieve DiD. The DiD approach integrates the capabilities of people, operations, and technology to establish multilayer, multidimension protection—much like the defenses of a castle. The "IA Through Defense in Depth" brochure was published in February 2000. It provides readers with the fundamental concept behind DiD and completes Phase 1 of the DID implementation strategy. Phase 2, publishing revised policy, is nearly complete. This new policy will be officially signed and published in December 2000. The primary objective of the revisions is to identify the minimum IA capabilities required for CINCs, Services, and Agencies (C/S/As). The C/S/As have identified and agreed upon 55 IA capabilities. Phase 3, publication of new policy, is anticipated to be completed in the third quarter of FY 2001.

The Information Assurance Panel's (IAP's) charter was rewritten in 1999 to bring several existing IA working groups under a single staff reporting to the Military Communications - Electronics Board (MCEB). The panel is cochaired by the JCS/J6K Division Chief and the Director of DIAP. It meets monthly with its C/S/A members and has become the focal point for IA-related issues within DoD. The high level of seniority of the Panel members has enabled the IAP to expand and tackle a host of critical IA issues this year. One of its most noteworthy accomplishments is the development of a DoD policy on the use of mobile code. The Panel's work led to a significant reduction in DoD's information and information systems' mobile code vulnerability. IA aspects of Defense Message System (DMS), Information Assurance Vulnerability Analysis (IAVA) compliance, international coalition accreditation authority, and Public Key (PK)-enabled applications are only a few additional examples of important IA issues addressed by the IAP this year.

IA Instructions and NETOPS

An important Joint Doctrine publication and the instruction governing IA are both under revision. The Joint Doctrine publication is being rewritten to focus on the concept of Network Operations (NETOPS). NETOPS is essentially the means through which the Global Information Grid (GIG) is run. NETOPS comprises three pillars: Information Assurance, Network Management, and Information Dissemination Management. The Joint Policy series will be a family of instructions providing NETOPS policy. Supplements to them (e.g., "Information Assurance Through Defense in Depth") specifying IA readiness reporting and other Computer Network Defense incident reporting will also be published.

IA Readiness Metrics

The Joint Staff published the IA Readiness Metrics Instruction in May 2000. It will help normalize IA readiness metrics into the Joint Monthly Readiness Report (JMRR) process. The plan is to render operational IA Readiness reporting not just for combat, combat-support, and combat-service units, but for all units. This will be achieved by integrating IA Readiness reporting into the higher-level component of the Operational Readiness reporting process.

Computer Network Defense Policy

The Joint Staff has worked with OSD and USSPACECOM on numerous documents defining Computer Network Defense (CND) and outlining associated roles and responsibilities. CND is a USSPACECOM mission that is a subset of Information Operations and tightly interwoven into IA. A strong working relationship between USSPACECOM and the Joint Staff's IA staff is fostering superior coordination among USSPACECOM, the Joint Staff, and OSD.

Joint Task Force IA Capability

The Joint Staff sponsored the pilot deployment of an IA capability to complement the network management capability already provided to the CINCs. The pilot program provides the Joint Task Force (JTF) Commander with the capability to monitor the IA status of the Area of Responsibility (AOR). The pilot program included components for monitoring the network, applications, and firewalls for intrusions. It also provided the capability to scan the network for known vulnerabilities and to report weaknesses. This pilot will be briefed to the IAP and MCEB for final approval as the Joint IA tool.

U.S. CENTRAL COMMAND

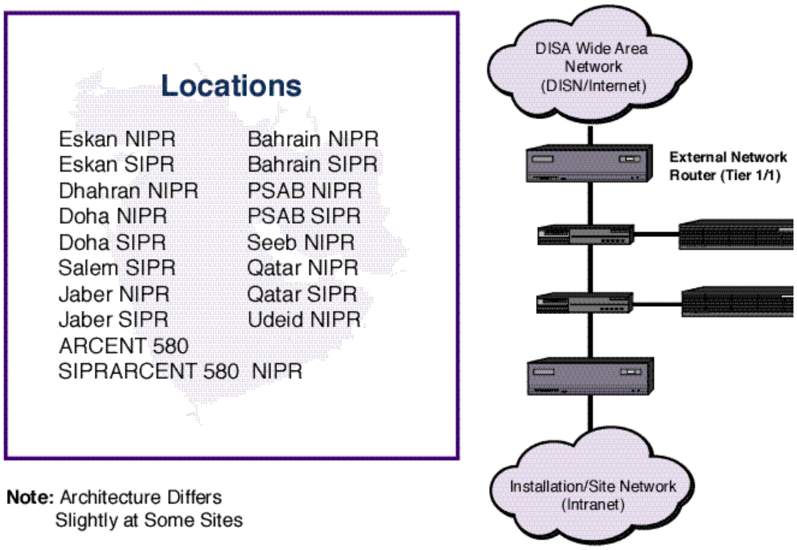
The United States Central Command (USCENTCOM), headquartered at MacDill Air Force Base in Tampa, Florida, is responsible for U.S. security interests in 25 nations, stretching from the Horn of Africa through the Arabian Gulf region and into Central Asia. USCENTCOM is one of nine Unified Commands in the Department of Defense. The Command was activated in January 1983 as the successor to the Rapid Deployment Joint Task Force. The Headquarters staff includes more than 900 personnel drawn from the four Military Services. Each of the Services also provides USCENTCOM with Component Commands that, along with the Joint Special Operations Component, constitute USCENTCOM's primary warfighting and engagement organizations.

IA Planning

In the area of accreditation and certification, USCENTCOM Information Assurance Branch (CCJ6-CW) developed and implemented an innovative plan to identify and correct computer network vulnerabilities and accredit Component sites throughout the AOR. Assisted by teams from the Defense Information Systems Agency (DISA) Field Security Operations (FSO) Office, USCENTCOM IA personnel traveled to 12 sites in 7 different countries to complete this task. Each site was visited three times in FY 2000 to ensure that new vulnerabilities were identified and corrected and to ensure IAVA compliance. Security for more than 6,000 computer systems was significantly improved by correcting more than 20,000 findings and by drafting accreditation packages for each site. The program and its success were briefed by video-teleconference to the Joint Staff Director of Command, Control, Communications, and Computer Systems (J6) and the J6 Directors of all Unified Commands for consideration for DoD-wide implementation.

The Command's Automated Information System (AIS) regulation is in the process of being updated to include the latest emerging technology security innovations. In addition to updating password configurations; network monitoring; and the introduction, removal, and accountability of new AIS equipment into and from USCENTCOM facilities, it includes appendices to address such issues as remote administration and router configurations, personal digital assistants, firewall policies, and IA vulnerability alerts. The regulation was also expanded to include AIS security beyond USCENTCOM Headquarters. It now encompasses Component Commands (NAVCENT, MARCENT, CENTAF, and ARCENT), Joint Task Forces, and elements deployed to the USCENTCOM AOR. In addition, an easy-to-use, web-based "Defensive Information Operations (DIO) User's Guide" was developed to educate systems administrators and individual computer users on how to protect their systems. Both the draft regulation and User's Guide are readily accessible at the USCENTCOM DIO

Typical Architecture



Note: Architecture Differs Slightly at Some Sites

Figure 30

SIPRNET website and have been widely used as a template by other Commands and Agencies.

The System Security Authorization Agreements and supporting risk assessments of all AISs within USCENTCOM Headquarters, USSOCCENT Rear, USNAVCENT Rear, and USMARCENT Rear were combined into a single site accreditation document that consolidated myriad systems into one package that is easier to manage and keep current. In addition, an exportable, easily understood, generic risk assessment package was developed to rapidly confirm the security status and risk assessment of deployed systems.

With the assistance of the 9th Information Warfare Flight, the Intrusion Detection System (IDS) hardware and software was upgraded throughout the USCENTCOM AOR, at Headquarters, and at Component sites located at MacDill AFB. These latest versions of software and hardware greatly improved perimeter network defense and allowed faster network speeds. The Automated Security Information System (ASIMS) version 2.0 was installed, in addition to the IDS installed at each site in the AOR, to provide an additional toolset for conducting forensic analysis of intrusion events. The ASIMS will be upgraded in 2001 to version 3.0 to provide an additional capability for active IP blocking similar to that already provided. The Air Force Computer Emergency Response Team (AFCERT) and the 9th Information Warfare Flight continue to monitor, control, and support these tools for USCENTCOM.

USCENTCOM and DISA implemented a Joint Staff-sponsored pilot program to integrate IA tools with network management systems in Saudi Arabia and Bahrain. This pilot program is designed to federate a suite of IA tools with the Joint Defense Information Infrastructure Control

System – Deployed (JDIICS-D). The pilot will also help in the development of an IA tool for Joint Task Force Commanders.

During the multinational exercise Bright Star 2000 (held in Egypt), USCENTCOM provided all deploying units with IDS and COTS routers to actively block hostile activity. NSA and DISA deployed to the exercise to test the strength of its network and train systems administrators on computer security. NSA and DISA scanned the network, using commercially available IA tools. Vulnerabilities were identified and corrected with the systems administrators. This security training was geared toward preparing USCENTCOM personnel to identify and defend against red team operations scheduled during exercise Internal Look 2001.

U.S. EUROPEAN COMMAND

The U.S. European Command (USEUCOM) is headquartered at Stuttgart, Germany. USEUCOM's mission is to maintain ready forces to conduct the full spectrum of military operations unilaterally or in concert with its coalition partners; to enhance transatlantic security through support of NATO; to promote regional stability; and to advance U.S. interests in Europe, Africa, and the Middle East.

Creating IA Awareness

In an effort to broaden IA awareness within the Command and the region, USEUCOM hosted its first IA Conference from 30 November to 02 December 1999 at the Abrams Center in Garmisch-Partenkirchen, Germany. The conference had three purposes: (1) to present pressing IA issues and review associated IA products, (2) to foster teamwork and synergy among key IA players in the theater, and (3) to provide the latest IA informational updates for theater IA personnel. By design, all levels of IA professionals, from enlisted to general officer grades (about 150 participants), engaged in the sessions. This arrangement ensured expression of various viewpoints at the forum and enabled individuals with hands-on experience to interact directly with policy makers at the highest levels. Operations discussions focused primarily on lessons learned from Kosovo operations and plans for future support. Participants dealt with IAVA issues and discussed the technical details of dealing with theater-specific threats. The communications security (COMSEC) sessions explored the areas of key management infrastructure, secure telephone equipment (STE) migration, Defense Message System (DMS) fielding, and Global Broadcast Service (GBS) fielding.

To ensure meaningful conference results, a Theater Action Team (TAT) was formed. Comprising key IA decision makers in the USEUCOM theater, the TAT met each evening to review and debate the many issues raised in the conference breakout tracks. After reviewing the issues, the team selected a subset of 20, ranked each by priority as high or medium, and assigned to each action a primary office of responsibility. As a result of its success, the conference led to the development of a new European Information Assurance Steering Council, comprising senior IA leaders and aimed at providing continuing, unified guidance to theater IA personnel. In addition, two working groups have been addressing each of the 20 action items for resolution.

IA Planning

One of the foundations of IA efforts in USEUCOM is the USEUCOM IA Master Plan. The IA Master Plan is a living, evolving document that identifies and coordinates the best DoD/Joint, Service, MAJCOM, and Component IA initiatives. The plan assesses the current IA environment, identifies a target architecture and implementation strategy, and sets forth specific action plans, with cost estimates, for resolution of major theater IA issues through FY 2004. During FY 2000, 13 action plans were followed to engage IA personnel and users, improve operational support, and improve the IA technology as part of USEUCOM's C4 modernization efforts. Plans included systems administrator training courses, end-user training, and certification and accreditation support for critical downrange networks, as well as the purchase of data transfer devices for COMSEC support, push-to-talk handsets for Command centers, and secure mobile telephones for USEUCOM theater senior leaders.

HQ USEUCOM has undertaken an initiative to identify all theater-critical telecommunications facilities and assess dependencies and vulnerabilities of military operations resulting from any possible disruption to key defense and commercial infrastructure Components. There are more than 50 accreditation efforts ongoing for all HQ USEUCOM systems, for which USEUCOM/J6 is the designated approval authority (DAA). In addition, Communications Interoperability and Security (CIS) Memoranda of Agreement (MOAs) have been developed with several nations within USEUCOM's AOR. These MOAs support increased interoperability with allies for mutual regional defense and potential combined operations.

An M-3 Bradley Fighting Vehicle in the cold snows of Bosnia.

More than 650 military personnel from 35 nations participated in the Combined Endeavor 2000 exercise that was held at Lager Aulenbach, Germany, 11–25 May 2000. An Information Systems testbed was used as a forum for technical presentations and demonstrations on the subjects of firewalls, PKI, intrusion detection, viruses, and hackers. Most of the nations in the test cell agreed to help in the IA evaluation by assigning an IA officer to complete two self-evaluation forms (one for workstations and one for servers). The results were used to demonstrate how to do a simple risk analysis and also to help all participants gain an understanding of where shortcomings might exist in coalition IA.

The Joint COMSEC Monitoring Activity (JCMA) continued to provide timely, prudent support to USEUCOM theater operations. This support has included Task Force Falcon in Kosovo, Task Force Eagle in Bosnia, Operation Northern Watch over Northern Iraq, and U.S. Sixth Fleet operations throughout the Mediterranean. By making communicators aware of nonsecure practices, JCMA reporting led to significant reductions in the amount of information disclosed inadvertently by U.S. Forces. Having shown the value it brings to operations, JCMA support became a standard part of all theater exercise planning.

Defense Information Systems Agency - Europe (DISA-EUR) support includes the operation of the European Computer Emergency Response Team (EURCERT). The EURCERT provides daily and weekly summaries of network intrusion reports, IAVA tracking and resolution assistance, and theater computer incident reporting to the DoD-CERT. It chairs the USEUCOM intrusion detection working group to synchronize technical assessments of computer incidents. In addition, the DISA Field Security Office (FSO) conducted security readiness reviews for USEUCOM networks in Germany, Turkey, and Belgium and for Task Force Eagle and Task Force Falcon, as well as an independent snapshot of the IA Readiness posture in the HQ USEUCOM IA Readiness Review. DISA IA Technology Analysis Center (IATAC) products and services were instrumental in the completion of the IA Master Plan and its associated action plans.

USEUCOM has worked to fully integrate IA into theater operations, C4 modernization efforts, and engagements by sponsoring the theater IA Conference and theater IA Senior Steering Council, coordinating theaterwide solutions sets, and documenting its theater strategy in the Theater IA Master Plan. The future includes efforts to implement an IA Element into a Theater C4ISR Coordination Center (TCCC); integrate IA into USEUCOM operational plans; foster PKI/common access card development; update USEUCOM's IA Directive on DoD guidance on the Global Information Grid (GIG), Network Operations (NETOPS), and IA metrics; and conduct threat assessments on critical infrastructure.

U.S. JOINT FORCES COMMAND

The United States Joint Forces Command (USJFCOM), formerly the United States Atlantic Command, was established in October 1999. Headquartered in Norfolk, Virginia, the Command is geographically responsible for the Atlantic region and functionally responsible for the development, training, and coordination of the joint operations throughout the Department of Defense.

IA STAFFING

One of USJFCOM's biggest IA challenges continued to be in the staffing and billeting area. IA civil service, military, and contractor staffing levels at USJFCOM continued to be insufficient for its IA strategic vision and goals. The USJFCOM IA Branch has a staff of 13 personnel who conduct information system security, IA training, and CND for Headquarters networks, as well as oversight for the IA programs of 17 subordinate Commands. Hiring caps and funding limitations did not allow creation of additional civil service billets or hiring additional contractor support.

To help overcome the IA staffing shortfall, the USJFCOM IA Branch employed one U.S. Air Force active reserve officer and incorporated the drill time of two U.S. Navy reserve officers, two U.S. Air Force enlisted reservists, and one U.S. Army enlisted reservist. These reserve personnel were used to assist in the installation of new IA systems onto USJFCOM's Headquarters networks and to generate SOPs for these systems.

Currently, USJFCOM IA Branch is working to get a Civilian Leadership Development program internist to help generate IA plans and policy and manage a consistent IA strategic vision across all its mission areas of Joint Force Provider, Joint Experimentation, Joint Training, and Joint Integration. Also, USJFCOM IA Branch has requested that DISA Field Security Office provide a dedicated, on-site Security Engineer to support IA systems engineering throughout Headquarters and subordinate Commands.

Using three existing personnel (one Chief Warrant Officer and two E-5 personnel), the USJFCOM IA Branch established a CND Cell, which is responsible for procuring, installing, operating, and maintaining IA systems for the Headquarters networks. The CND Cell generates SOPs and provides training for the System Operations Center (SOC) watch team, who monitor all the Headquarters networks, as well as its IA systems. The CND Cell also participates in the DISA Joint Program Office's Advanced Concept Technology Demonstrations (ACTD), testing new IA systems. During crisis action periods, the CND Cell is augmented by senior IA Branch personnel and supports the Joint Planning Group, Crisis Action Team, and Information Operations Cell on a 24-hour watch rotation.

To augment the SOC watch team, USJFCOM IA Branch developed a plan for a 10-member CERT. Once established, the USJFCOM CERT would monitor Headquarters IA systems and networks in order to prevent, detect, react to, and report network security violations, intrusions, or attacks. An unfunded budget request was submitted for this CERT.

IA Training

USJFCOM IA Branch was able to take advantage of DISA-provided training on Web Security and on Enterprise Security Manager/Intruder Alert (ESM/ITA) software, to further educate CND Cell analysts. CND Cell analysts also attended systems administrator training courses in the local community. In addition, the Navy's Fleet Information Warfare Center (FIWC) provided the IA staff with computer security training.

USJFCOM IA Branch worked with the Joint Warfighting Center's Information Operations (IO) Planning Cell to incorporate additional IA focus into Joint Task Force training exercises. Changes in Information Operations Conditions (INFOCONs), as well as red team simulations, are currently included in these exercises. In addition, the Joint C4ISR Battle Center, a USJFCOM CINC activity, in coordination with the Joint Warfighting Center and USJFCOM J9 (Joint Experimentation Directorate), introduced new IA technological and systems capabilities into the USJFCOM's first joint experimentation event, "Millennium Challenge 2000" (MC-00) to obtain warfighter feedback on the systems' operational utility and concepts of operation for the deployed joint force. The vision for future exercises includes actual, vice simulated, attainment of INFOCON actions to train operators on backup communications, procedures, contingency plans, and realistic CND scenarios to support refinement of CONOPS and joint tactics, techniques and procedures.

To supervise operation of USJFCOM's Local Information Management System (LIMS), GCCS, JIDS, FRRS, JTAV, and JRAMS Classified systems, USJFCOM has 55 Level 1 certified systems administrators.

USJFCOM concurred with the Joint Staff Directive for the Implementation of the Recommendations of the Information Assurance and Information Technology Integrated Process Team on Training, Certification, and Personnel Management in the Department of Defense. The recommendations will significantly enhance the necessary training for systems administrators.

USJFCOM is working closely with DISA in providing the staff and subordinate Commands with DISA-funded Level 2 systems administrator training. The first round of training was conducted on COTS Security 04–08 December 2000 at USJFCOM. The course is designed to help the beginning-to-advanced systems administrators understand what constitutes a secure system and what tools exist to provide assistance in the day-to-day task of monitoring and securing the network. This course has been approved as meeting the training requirements for systems administrator's Level 2 certification for C2-level security by DISA. Training dates for Security Level 2 are to be determined. A request for attendees was sent out to USJFCOM Commands in the local area.

USJFCOM encouraged and made recommendations to all its subordinate Commands to meet ASD(C3I)'s and the MECB's deadlines for certifying systems administrators. All Classified network administrators were to be certified by 31 December 1999. Systems administrators of Unclassified and all other DoD networks are to be certified by 31 December 2000. Subordinate Commands were tasked to report the status of systems administrator certifications to USJFCOM at the end of the fiscal year. Included in this message were the requisite skill levels and certification requirements for all three levels of systems administrators.

Annual security training, to include automated information systems security, physical and information security, operations security (OPSEC), and antiterrorism/force protection (AT/FP), was provided to the entire USJFCOM staff in May 2000. This one-stop, consolidated training session was mandatory for all military and civilian personnel and was also offered to all contractor personnel. Users received handouts to keep and use as a ready desk reference.

Quarterly training is provided to all directorate Information System Security Officers (ISSOs) to keep them abreast of the latest changes in information systems security and make them viable extensions of the IA Branch for enhanced security support throughout the Headquarters staff.

USJFCOM IA Branch implemented new banner page software to provide IA situational awareness and security alert information to network users upon login to Headquarters networks. These multiple login banner pages are changed weekly to reflect current IA issues and as policy refreshers on a constant basis. USJFCOM IA Branch also implemented System Security Alert e-mail messages sent to network users in the case of system vulnerabilities or a virus threat that users must be aware of.

IA Awareness

USJFCOM IA Branch participated in U.S. Space Command's INFOCON Conference and provided recommended minimum direction actions for all Commands to take upon setting a particular INFOCON level. These actions included user education, watch team augmentation, and network configuration changes.

USJFCOM subordinate Commands were directed to evaluate the Joint Staff's IA Readiness Metrics in their command, control, communications, and computers (C4) section of their Joint Monthly Readiness Review (JMRR). Starting with the October 2000 JMRR, subordinate Commands are reporting the status of IA plans and operations, IA training, and IA resources and enablers. USJFCOM IA Branch will use this information not only to generate its C4 JMRR input but also to identify subordinate Commands requiring additional assistance in improving their IA programs.

Scott Air Force Base's CERT now works directly with the USJFCOM SOC to notify the Command of system vulnerabilities or virus threats. This has allowed quicker actions to protect our networks and eased Scott CERT's notification procedures.

The USJFCOM IA Branch initiated the generation of an Address Indicator Group of its subordinate Commands to allow the Joint Task Force for CND (JTF-CND) and DoD CERT to directly notify all USJFCOM Commands of system threats. This negates the need to readdress message traffic to subordinate Commands and greatly speeds up network protection response time

IA Readiness

Efforts are underway to ensure that all USJFCOM information systems comply with the mandated DoD Information Technology Security Certification and Accreditation Process (DITSCAP) for certification and accreditation. All systems and networks must provide appropriate accreditation documentation before being connected to the USJFCOM infrastructure. All accreditations and Interim Authorities to Operate (IATOs) are tracked and suspensed for action to ensure that USJFCOM networks [SIPRNET, Local Information Management System (LIMS), and Global Command and Control System (GCCS)] remain in an accredited status.

During FY 2000, the USJFCOM IA Branch conducted Inspector General staff assistance visits (SAVs) and inspections at 6 of its 17 subordinate Commands. New Commands to USJFCOM received SAVs within the first six months in order to provide them with information and standards to prepare for upcoming inspections. Subordinates were inspected in the areas of Information Assurance, Information Systems Security, Global Command and Control System Security, Multilevel Security, and IA Training. The USJFCOM IA Branch provided assistance to the subordinates in correcting any identified issues.

USJFCOM established periodic IA Readiness Reviews (IARRs) of its five Subunified Commands and eight subordinate Joint activities. The DISA Field Security Office performs the IARRs and provides direction and assistance in correcting any identified deficiencies. The IARRs are assistance visits only and not used by USJFCOM as an inspection method. The results of the IARRs are kept internal to the Command and are not reported by DISA to USJFCOM

Headquarters. Each subordinate Commander is encouraged, however, to notify USJFCOM Headquarters of any assistance, resources, or training required to correct his or her Command's deficiencies.

On 01 July 2000, USJFCOM initiated the use of DISA's Vulnerability Compliance Tracking System (VCTS). Systems from USJFCOM Headquarters, Subunified Commands, and Joint activities are all registered on VCTS, and systems administrators receive e-mail reports from VCTS on IAVAs that impact their systems. Systems administrators report compliance directly to the VCTS websites, and the IA Branch monitors Commandwide acknowledgement and compliance with the IAVAs through executive accounts on the VCTS websites.

In preparation for the conversion to VCTS, USJFCOM provided (1) on-site and video training on VCTS websites and (2) procedures to Headquarters and subordinate Command systems administrators and IA staffs. USJFCOM also generated a VCTS procedures manual to assist the subordinate Commands in implementation.

An army UH-60 helicopter lands on the deck of a Navy ship.

USJFCOM received Command and Control Initiatives Program (C2IP) funding from the Joint Staff and procured Intrusion Detection Systems (IDSs), ESM/ITA systems, and a vulnerability scanner for installation on Headquarters networks. The CND Cell has received these systems and is in the process of testing and installing them on USJFCOM networks. The ESM provides security policy checking (e.g., password length, registry settings); ITA provides automated review of audit logs for unauthorized access. ESM/ITA will alert the CND Cell and SOC to any unauthorized access to network servers. The vulnerability scanner will allow the CND Cell to internally test the security configurations of USJFCOM networks.

USJFCOM worked closely with DISA to plan for the upcoming installation of audit servers on Headquarters networks. The audit server will permit expanded archiving of audit logs from multiple servers and has a jukebox to write and store long-term audit data on CDROM.

USJFCOM's CND Cell is in the process of installing IDS on its Headquarters networks. These IDS tools will augment the Joint Intrusion Detection Systems (JIDS) already in place and monitored by Scott CERT and will allow the CND Cell and SOC to perform real-time monitoring of USJFCOM Headquarters networks under the noise level of Scott CERT.

USJFCOM is currently working with DISA Field Security Office to implement the Fall 2000 installation of redundant firewalls on its Classified network and of additional firewalls on its Unclassified network. It is also working with the DISA Field Security Office to obtain and install additional JIDS suites on subordinate Command networks and deployable tactical systems.

USJFCOM is currently installing redundant Headquarters SIPRNET connections that will allow automated fail-over and keep critical command-and-control systems and information available to the Joint warfighters, experimenters, and trainers. USJFCOM is currently implementing PKI encryption on its Unclassified web servers and planning for further expansion of PKI use in the next two years.

USJFCOM continues to participate in DISA JPO's IA-related ACTDs to evaluate new ideas and technologies that will improve CND operations. USJFCOM participated in a minidemonstration of the Automated Intrusion Detection Environment (AIDE), ACTD, as did the JBC. The JBC also conducted a mini-assessment of the AIDE system in conjunction with their FY00 assessment of new IA technologies for the deployed JTF in MC-00.

During FY2000, the JBC's IA assessment team completed its second formal assessment of new IA technologies for the deployed Joint Task Force (JTF). The project, entitled the "Joint Task Force Network Security Management (JTF-NSM)" assessment was approved by the Joint Staff and Unified Commanders in Chief (CINCs) as a formal JBC assessment based on the established JBC project selection process.

The FY00 project consisted of an independent assessment of a commercial enterprise security management system called "SAFESuite," selected by DISA and sponsored by the Joint Staff J6 for evaluation as candidate IA (intrusion detection, vulnerability assessment, event correlation, reporting and decision support) capability to accompany the distribution of the JDIICS-D interim joint network management system. The commercial suite, designated by DISA as the "IA Components for JDIICS-D Pilot," was assessed by the JBC to determine its maturity, jointness, and value-added utility to the deployed force, and to capture and document operational issues relative to the system's implementation in the joint tactical architecture.

The JBC assessment incorporated all three phases of the JBC's formal assessment process, including an in-lab "desktop assessment" conducted by JBC technicians and subject matter experts (SMEs); assessment during a joint collaborative experimentation phase with CINC, Service and agency SME and warfighter participation; and an assessment during a joint exercise or as in this year's case, a joint experimentation event, to gather warfighter hands-on feedback.

In conjunction with this assessment, the JBC identified and addressed IA, CND, and network security management Concept of Operations (CONOPS), Tactics, Techniques, and Procedures (TTP), network security policy, and manpower and training shortfalls, in order to recommend near-term courses of action believed necessary for successful implementation of these capabilities on deployed tactical networks. Much of this information was formally incorporated into a draft Joint IA CONOPS, developed by the JBC in conjunction with CINC, Service, and Agency (C/S/A) working groups, under the auspices of the Joint Staff J6K, entitled the "IA/CND Element of the JTF NETOPS CONOPS." Findings, conclusions and recommendations stemming from the JBC assessment and the development of the CONOPS will be delineated in a formal assessment report, and briefed to the DoD IA Panel, DISA, the Unified CINCs, the Joint Staff J6K, the Military Communications and Electronics Board (MCEB), the Theater Joint Tactical Networks Configuration Control Board (TJTNCCB), the Joint Network Management System Program Management Office (JNMS PMO), and other Joint, Service, and agency organizations in effort to gain consensus and synergy on issues relevant to the rapid insertion of new IA capabilities into the joint tactical architecture, and accelerated establishment of IA interoperability across the Global Information Grid (GIG).

In addition to the assessment of the IA Components for JDIICS-D, the JBC served as an official sponsor for the FY00 Joint Warfighting Interoperability Demonstrations (JWID), wherein several new IA technologies were demonstrated. The JBC IA assessment team supported the JWID Joint Program Office and designated JWID assessment personnel by providing SME input relative to the IA technology demonstrations, including this year's JWID "Gold Nugget" winner, "SilentRunner."

During FY01, the IA Branch and the JBC will work closely with other JFCOM staff elements to introduce findings, conclusions and recommendations from involvements in ACTD demonstrations, JWID, joint experimentation, and JBC assessments into pertinent focus areas such as the GIG IA architecture and Capstone

Requirements Document (CRD), in effort to expedite insertion of near-term technological capabilities into the deployed systems and operational architectures and expedite attainment of information superiority.

U.S. PACIFIC COMMAND

The United States Pacific Command (USPACOM), headquartered at Camp H.M. Smith, Hawaii, is responsible for promoting peace and deterring aggression throughout the Asia-Pacific region. This region includes 48 countries or entities and 105 million square miles—more than half of the Earth's surface.

For FY 2000, Commander in Chief, Pacific (CINCPAC) recognized the criticality of IA and continued to develop healthy, aggressive programs throughout the USPACOM AOR. In planning the USPACOM prototype Theater Network Operations and Theater C4ISR Coordination Center (TCCC), IA played a major role in its development. The TCCC provides the systems and network situation awareness necessary to effectively manage

A Marine Heavy Helicopter Squadron 464 (HMH-464) CH-53E Super Stallion helicopter lands on the flight deck of the amphibious transport dock USS RALEIGH (LPD-1) as other ships of the amphibious task force steam in formation behind.

reliable and secure voice, data, and video services within a theater. Making IA an intrinsic part of all its Information Operations (IO) has enabled USPACOM to think out and develop its IA capabilities in advance, rather than react to crisis situations.

A guided missile frigate slowly cruises while accomplishing its undersea warfare mission.

USPACOM has expanded its IA operations considerably during this fiscal year. The first major effort was the Y2K turnover, which it successfully negotiated with no major impact to its systems. USPACOM established a permanent 24x5 IA position in the USPACOM Theater C4ISR Coordination Center (TCCC). In addition, it developed and implemented a process for the dissemination and compliance tracking of Information Assurance Vulnerability Alert (IAVA) and Information Assurance Vulnerability Bulletin (IAVB) information to USPACOM Components, Subunified Commands, and Joint Task Forces (JTFs). Upon receipt of IAVAs and IAVBs, USPACOM exercises prompt information dissemination to all Commands and Subunified Commands. The Commands and Subunified Commands are required to acknowledge receipt of the message within 5 days and to become compliant within 30 days. USPACOM ensures compliance by following up with specific commands for status on current activity in relation to the IAVAs/IAVBs. The past fiscal year yielded six IAVAs and seven IAVBs.

USPACOM coordinated with the Joint Task Force - Computer Network Defense (JTF-CND) on actual computer virus incidents such as the "ILOVEYOU" virus. The TCCC facilitated this effort by ensuring that all Components were using the latest antivirus software and had in place preventive measures to prevent further contamination. In concert with that effort, TCCC continued to provide in-depth analysis of CERT computer incident reports and to conduct daily IA briefings on theaterwide IA activities. This briefing serves as an effective trend analysis tool, whose analytical results are targeted at the CINC level. USPACOM participated in four major theater exercises—Reception, Staging, Onward Movement, and Integration (RSO&I) 1999; RSO&I 2000; Ulchi Focus Lens (UFL) 2000; and Ellipse Charlie (EC) 2000—as well as several internal and Command exercises. Along with this on-the-job training, it facilitated IA training, vulnerability assessment, and a certification computer-based training program in conjunction with other OSD initiatives for USPACOM personnel.

U.S. SPECIAL OPERATIONS COMMAND

United States Special Operations Command (USSOCOM), a unified command headquartered at MacDill Air Force Base, Florida, directs approximately 47,000 active duty and reserve component personnel in the Army, Navy and Air Force under a single commander. USSOCOM is responsible for preparing special operation forces for worldwide special operations, civil affairs and psychological operations in peace and war in support of regional combatant commanders and other government agencies.

With the ever-increasing dependence on computer-based communications platforms, the need to protect Special Operations Command (USSOCOM) information has become even more critical. Networks that interconnect with the Special Operations Force (SOF) need to be protected at the local enclave level, as well as through the transmission path. Information confidentiality, authenticity, integrity, nonrepudiation, availability, and clarity are just as important in the battlefields, today and tomorrow, as in the past.

IA Goal

USSOCOM has put much effort into its IA operations and has drawn from many of its lessons a series of overarching goals. These goals form the basis of USSOCOM planning, development, and function and are the basic premises of its IA posture. Coupled with the operational aspects of IA, these goals (listed below) provide the means to protect and defend the information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation:

- **Goal 1.** Increase information throughput for deployed forces. Required in support of improved situational awareness for SOF Commanders, teams, aircrews, and water crews. Provide the high bandwidth path to pass imagery of target locations, UAV video and sensor feeds, location of enemy/friendly forces, status of support missions, satellite sensor broadcasts, etc. Provide information on demand to the deployed team, and download it to a man-packable system.
- **Goal 2.** Provide common information interfaces and services across all echelons of SOF, including team-level communications and mobile system platforms.
- **Goal 3**. Maximize SOF connections to the Global Information Grid (GIG). Leverage DoD-wide efforts to globally interconnect capabilities, processes, and personnel for collecting, processing, storing, and disseminating information, on demand, to the war fighter.
- **Goal 4.** Reduce the size, weight, and type of information systems required. Focus on quality versus quantity of information technology systems in their inventory, and

standardize wherever possible across the Command to minimize operational and logistics expenses.

- **Goal 5.** Reduce the forward footprint of SOF by providing direct, on-demand, real-time linkup between the special operator in the field and rear echelons.

During the past year, USSOCOM, using firewalls and intrusion detection systems, has enhanced the security of the networks, both in-garrison and deployed. Firewalls were added as a second level of protection between the internal and external networks, and IDSs provide additional detection of inside and outside threats.

Making Use of IA Technology

To protect its e-mail systems, USSOCOM uses antivirus and e-mail attachment filtering programs. It installed COTS applications to prevent insider and outsider threats from accessing the internal network. USSOCOM IA purchased and implemented COTS network scanning software, giving the IA Branch technicians the ability to check all the servers and clients on all networks. In addition, a COTS software suite will be used to enforce established policies. The network security enclave was strengthened by adding the Joint Intrusion Detection (JID) system to warn of ongoing unauthorized activity on the Classified and Unclassified networks.

Low crawling through the mud and under razor wire.

In September 1999, the HQ USSOCOM Network Operations Security Center (NOSC) became fully operational by colocating similar functions into a single center. The NOSC actively monitors network flow and unauthorized monitoring of the networks and quickly responds to threats. The NOSC also provides for rapid reporting of suspicious network-related events to regional and national network security operations centers. It was instrumental in ensuring the smooth transition during the Y2K rollover.

The Special Operations Intelligence and Information Operations (SOIO) Center completed a major reorganization by grouping together similar security and information protection functions. SOIO-SI (Information Assurance) has been tasked to provide a single USSOCOM-wide perspective. To perform this task, it has taken a worldwide focus with national-level coordination. This worldwide focus has allowed USSOCOM to leverage the Defense Information Systems Agency (DISA) support down to SOF Components and to participate in CND exercises such as Apollo CND.

The SOIO-SI performs the key missions of policy development, technical security, vulnerability testing, training and certification, communication security (COMSEC), and research and development. It coordinates the performance of these IA missions with USSPACECOM, NSIRC, DoD CERT, Service CERTS, JTF-CND, and DISA Regional NOSC.

The USSOCOM IA program policies were promulgated to provide a roadmap for securing and maintaining the networks. The Technical Security Section has started an aggressive technical review of the Command's networks and special programs to ensure network survivability and integrity. This review, along with the cited policies and procedures, sets the stage for successful certification and accreditation of the Command's networks.

To further enhance the network's overall security profiles, USSOCOM initiated an ambitious multiyear, concentrated blue team/red team inspection cycle. The Command's user certification/recertification program and the increased emphasis on network vulnerabilities during annual security training has increased the overall security awareness of the Command's personnel. The STU-III to STE migration program, along with the PKI initiative, continues to chart more robust and secure communications life-cycle management from garrison down to the deployed teams.

Through USSOCOM's Systems Engineering Technical Assistance contract, USSOCOM augmented Service SOF Components (Joint Special Operations Command, Air Force Special Operations Command, Army Special Operations Command, and Naval Special Warfare Command) with 11 additional IA contractor personnel.

U.S. SPACE COMMAND

The U.S. Space Command (USSPACECOM) Headquarters and the North American Aerospace Defense Command (NORAD) are colocated at Peterson Air Force Base, Colorado. NORAD is a binational, American-Canadian organization charged with the missions of aerospace warning and aerospace control for North America. Aerospace warning includes the monitoring of man-made objects in space and the detection, validation, and warning of attack against North America, whether by aircraft, missiles, or space vehicles, using mutual support arrangements with other Commands. Aerospace control includes providing surveillance and control of the airspace of Canada and the United States.

USSPACECOM, one of nine combatant Unified Commands of the United States, coordinates the use of Army, Naval, and Air Force space forces to perform the following missions:

- **Space Forces Suppor t** – Launching and operating satellites
- **Space Force Enhancement** – Supporting Joint Service military forces worldwide with intelligence, communications, weather, navigation, and ballistic-missile-attack warning information
- **Space Force Application** – Engaging adversaries from space
- **Space Force Control** – Assuring U.S. access to, and operation in, space—and denying enemies that same freedom
- **Computer Network Defense** for the DoD effective 01 October 1999; on 01 October 2000, USSPACECOM assumed the additional DoD mission of Computer Network Attack

The J6 staff supports both Commands. While the Commands' missions are distinct, the necessary staff support for one Command frequently overlaps that of the other. For this reason, the Information Assurance Report input for NORAD-USSPACECOM is submitted as a joint effort.

Figure 31 depicts the organization that these Commands are using for Information Operations and Information Assurance.

These three rings show the current NORAD-USSPACECOM structure and organization to plan and execute Information Assurance and Information Operations. This structure was built to help address the following common issues between the two Commands:

- The NORAD-USSPACECOM Core CND Cell comprises representatives from the Operations, Intelligence, Plans, and Communications Directorates. These personnel manage day-to-day execution of the Commands' IO responsibilities for both Operations Directors.

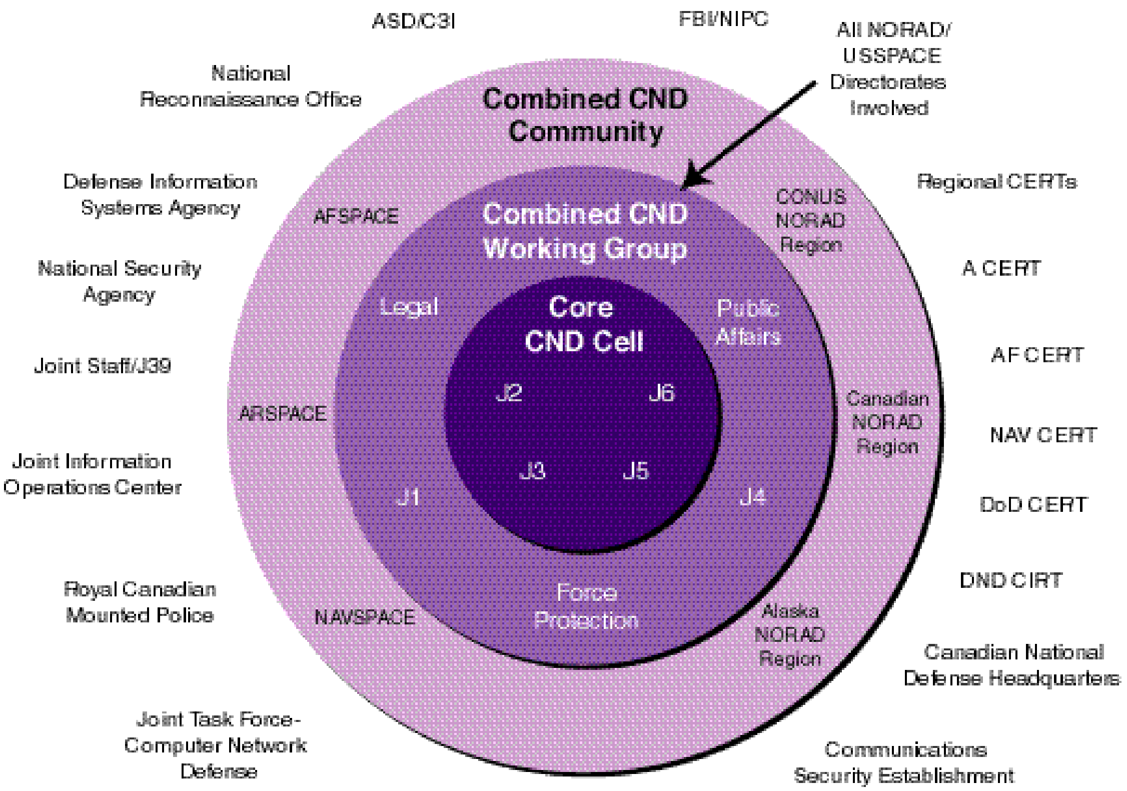

ASD/C3I
FBI/NIPC
All NORAD/ USSPACE Directorates Involved
National Reconnaissance Office
Combined CND Community
Defense Information Systems Agency
AFSPACE
Combined CND Working Group
CONUS NORAD Region
Regional CERTs
National Security Agency
A CERT
Legal
Core CND Cell
Public Affairs
Joint Staff/J39
AF CERT
J2
J6
ARSPACE
Canadian NORAD Region
NAV CERT
Joint Information Operations Center
J3
J5
J1
J4
DoD CERT
DND CIRT
Royal Canadian Mounted Police
NAVSPACE
Force Protection
Alaska NORAD Region
Canadian National Defense Headquarters
Joint Task Force-Computer Network Defense
Communications Security Establishment

Figure 31. NORAD-USSPACECOM IO/IA Organization

- The Combined CND Working Group augments the CND Cell and integrates the remaining HQ staffs, when required.
- The Combined CND Community adds the NORAD Regions and USSPACECOM Component forces.
- HQ NORAD-USSPACECOM routinely effects coordination with the external Headquarters and Agencies shown outside the rings.

IA Efforts

The first quarter of FY 2000 was focused on preparing for the critical Y2K rollover dates, principally 31 December 1999 to 01 January 2000 and the leap year dates of 28–29 February 2000 and 29 February to 01 March 2000. NORAD and USSPACECOM J6 formed a Command System Assessment Team (CSAT) to provide technical support to both Commands' operations centers on a 24x7 basis from 31

December to 3 January and during the Leap Year dates as well. Detailed contingency plans were developed for workarounds to any possible system outage or degradation. In addition, a system configuration database was developed for all NORAD and USSPACECOM mission strings, detailing all mission-critical information systems and how they were networked and routed from each sensor through the various operations and correlation centers to Cheyenne Mountain Operations Center (CMOC) and on to the National Military Command Center (NMCC); Canadian National Defence Operations Center (NDOC); and the other CINCs, Agencies, and forward users. This allowed the CSAT to quickly assess the impact of any Y2K outage, coordinate with the appropriate service provider or System Program Office (SPO), and provide the operators with an assessment of risk to the overall mission impact. No outages were reported.

Much of the effort during the Y2K effort was rolled into the Commands' IA work. The work completed on defining mission-critical systems and Command architectures was used as the starting point in network mapping and in identifying nodes for critical infrastructure protection. The system databases were used as the basis for the IT Systems Registration Database and as a tool to track system configuration control actions.

USSPACECOM conducted many exercises that allowed it to gain valuable hands-on IA training for its personnel. Apollo CND was the USSPACECOM exercise run simultaneously with the USCINCPACE/Combined Forces Command Reception, Staging, Onward Movement, and Integration (RSOI) 2000 Exercise, 14–20 April 2000, which had the following four goals:

- To exercise the C2 structure for Computer Network Defense
- To demonstrate CND operations proof of concept for the Uniform Joint Task List (UJTL)
- To allow USCINCSPACE and JTF-CND to test and refine their draft plan for the defense of the Defense Information Infrastructure (DII)
- To allow USCINCSPACE to continue development and refinement of CND relationships with the C/S/As and civil authorities

Other exercises completed were Vigilant Overview 2000, Apollo Lens 2000, Vigilant Condor 2000, Apollo/Vigilant Guardian 2001, Apollo Force 2001, and Joint Warrior Interoperability Demonstration (JWID) 2000–2001. One of the goals of the JWID exercise was to demonstrate enhanced information superiority technologies in a combined/coalition environment. Four JWID demonstrations supported this goal and included these operations:

- Silent Runner. Information network assurance demonstration (IDS inside and outside networks) and monitoring for intrusion detection

- C4ISR Systems. Reliability, performance, and situation awareness
- Telewall. Enterprise control of unauthorized modems, fax line misuse, and private branch exchange (PBX) fraud
- Space and Information Analysis Model (SIAM). Analyzed information flow on the battlefield to determine target priorities and information degradation from effects-based targeting (SIAM displayed communication paths, identified choke points, prioritized targets, analyzed strategies/courses of action, and identified intelligence collection shortfalls.)

USSPACECOM has sought greater coordination with the Joint Staff, other CINCs, and Agencies. Throughout the Y2K preparation and rollover time periods, NORAD and USSPACECOM and each Command's Regions, Components, and Subordinate Commands worked closely with DISA to ensure that there were no major problems with communications networks. Had there been problems, a method was in place to minimize mission impact and quickly restore any affected network to full capability as soon as possible. In addition, DISA worked with NORAD-USSPACECOM J6O to review the Defense in Depth (DiD) architecture of the Command-and-Control Automation System (C2AS). In particular, the DISA-USSPACECOM team reviewed the placement of intrusion detection systems, which the DISA RCERT at Scott AFB monitors for USSPACECOM.

The relationship between CINCSPACE and DISA was established by a Chairman of the Joint Chiefs of Staff Instruction and formalized by a CINCSPACE-DISA MOA signed December 1999. It is working well. DISA's D314, DISN Space Operations, is the organization vested by Director, DISA with responsibility to serve as Defense Satellite Communications System (DSCS) Satellite Systems Expert (SSE) and Commercial Satellite Communications Initiative (CSCI) SSE. The DSCS SSE role is shared between the DSCS Program Management Office and the DSCS Network Management Office.

Computer Network Defense

SP/J39 has worked to integrate the CND mission into USSPACECOM operations and planning considerations. INFOCON has been one of the major focus areas to ensure that all CINCs' IA postures are standardized and applied consistently across the range of conditions. IAVA compliance was reviewed throughout this process, with an eye toward "operationalizing" it to attain more complete compliance across the board. The process of validating TSABI/SABI should be tied to the operational mission. SP/J39 has worked closely with J37 and J6O to include new policy, procedures, and concepts for IA and CND into

Command exercises in order to validate and test them as they are developed. Work is also ongoing to update existing plans with IA/CND information, as well as the development of a CND OPLAN. An internal operating plan was published, providing the Headquarters with updated network security operating procedures.

The Mission Area Working Group (MAWG) hosted by USSPACECOM in March 2000 began laying out the long-range plan for CND until 2020. This included producing an Integrated Priority List (IPL), a mission needs statement, and critical requirements documents. As part of this process, the MAWG helped to develop Computer Network Defense/Attack (CND/A) Capability Roadmaps and CND/A FYDP Capabilities/Shortfalls for the 2003–2007 IPL, to align the ADEPT plan with the CND/A Plan, and to integrate the CND/A Plan into the space planning and requirements system. Conference attendees built the capabilities and the goals for both CND and CNA and then filled in the system technologies, policies, Concept of Operations (CONOPS), partnerships, and organizations required to meet the goals. The attendees followed the assessment of the overall roadmap and development of the 2020 IPL.

At the NORAD Mission Area Analysis Conference held in May 2000, Information Superiority became an independent area for the first time. Eleven desired operational capabilities were drafted for inclusion in the 2000 NORAD Mission Area Assessment Report, some of which directly and/or indirectly supported Command IA goals (such as the need for network mapping and the automated tools to accomplish it).

An interior view of a NORAD Command Post.

NORAD formed the Command System Assessment Team (CSAT) to manage Y2K events. Even though all the mission-critical NORAD and USSPACECOM systems and networks had been thoroughly tested and operationally evaluated (OPEVAL) before the actual Y2K rollover dates, steps were taken to have plans and personnel in place during the rollover dates to recognize, control, report, and coordinate correction of any problems that might arise. The CSAT was a team of technical experts assembled to provide technical support to both Commands' operations centers by providing risk assessment and mission impact evaluations should a problem occur during the Y2K rollover. The team was networked with all the Commands' Regions, Components, and subordinate Commands and the system program offices responsible for the mission-critical systems. This would ensure that information could be quickly shared and solutions to problems quickly found. Even though the CSAT encountered no problems during the rollover dates, much was learned that was applied to IA operations after the Y2K transition was completed.

The Joint Computer Coordination Center (JCCC) represents a continuation of the success of the Command System Assessment Team. The original idea was to form a team within NORAD-USSPACECOM J6 to provide technical support for network operations (computer and system networks) to the operations centers of USSPACECOM and NORAD. The JCCC will maintain day-to-day liaison with the J6/network personnel of all the NORAD regions and the USSPACECOM Components and subordinate Commands. With a constant dialogue between the J6s and their counterparts of the C/S/As, the objective is to be able to share network information on a real-time basis to cut across the vertical reporting chains of units to network centers to service CERTs. The goal is to be able to provide the CINC with an up-to-date status of all mission-critical networks and help the operators determine mission impact should an attack or failure occur.

Headquarters NORAD-USSPACECOM developed an Information Assurance Concept of Operations (IA CONOPS), which provides the overarching direction required to protect the Command's information networks. The CONOPS describes the NORAD-USSPACECOM focus and objectives for IA. In addition, the CONOPS identifies roles and responsibilities related to protecting NORAD-USSPACECOM information and information systems from unauthorized activity and describes the actions required to provide to the CINC a common operational picture of network status. Finally, the CONOPS provides background information on the perceived threats to NORAD-USSPACECOM Information Systems (IS). The CONOPS provides direction and establishes procedures to manage risk to the NORAD-USSPACECOM information infrastructure.

HQ NORAD-USSPACECOM J6 developed an approach for achieving Information Assurance (IA) of its Command-and-Control Automation System (C2AS) LAN through Defense in Depth (DiD). DiD is in part accomplished by establishing multiple means of protection in a series of physical and virtual layers through which information must pass. This ensures multiple ways of identifying and correcting information/network security problems before, during, and after their occurrence. The goal of DiD is to protect both the C2AS LAN and the information residing on it. The DiD strategy comprises many separate but interconnected parts. Each part is necessary and depends on each of the other parts for overall success.

The Vulnerability Compliance Tracking System (VCTS) was implemented at Headquarters NORAD-USSPACECOM in August 2000. IAVAs are now delivered directly to the systems administrators who can immediately take corrective actions.

All C2AS account users were trained and tested in security procedures for using the LAN. The training covered subjects such as password policies and requirements, security labeling for e-mails, and procedures for transferring files between systems. Network access was withheld for personnel who did not complete the training successfully by 30 November 1999.

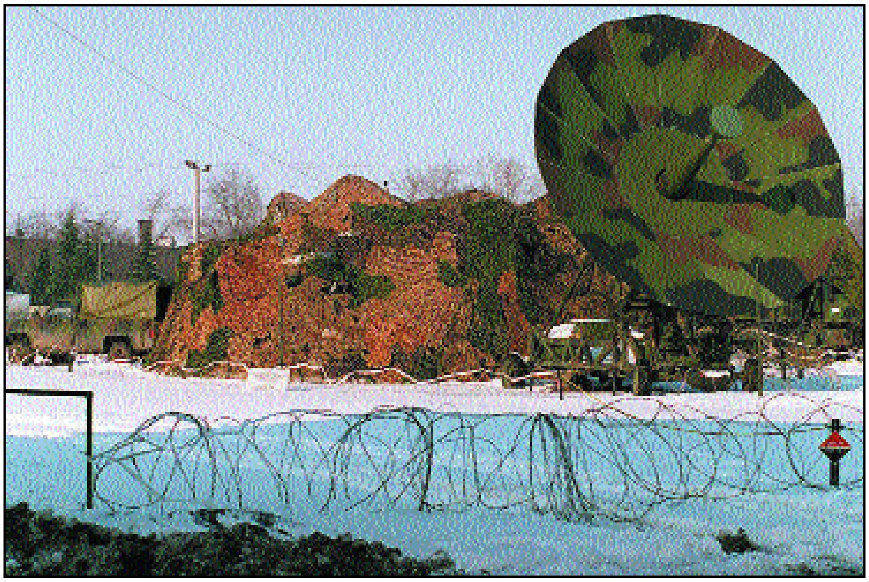
The Canadian NORAD Region (CANR), headquartered at Winnipeg, Manitoba, developed and implemented an IA Concept of Operations (CONOPS) and is regularly conducting training. In addition, that Command is currently forming an Intrusion Detection Plan.

Alaskan NORAD Region (ANR), headquartered at Elemendorf Air Force Base, Alaska, responds to guidance not only from NORAD, but—as 11th Air Force—also from HQ Pacific Air Force and Alaskan Command (ALCOM). This example of a single Command supporting more than one senior Headquarters underscores the need for top-level coordination of IA requirements/guidance among the CINCs, so that subordinate Commands are not inadvertently required to perform different tasks in response to the same situation.

CONUS NORAD Region (CONR), located at Tyndall AFB, Florida, is also HQ 1st Air Force, an Air National Guard organization that belongs, administratively, to Air Combat Command. This Command has an active IO Cell as part of its staff. The cell operates under an MOA among the various Air Combat Command directors that lays the ground rules for IO Cell functions. The CONR IO Cell developed and distributed to every CONR staff member a Computer Network Emergency Response Aid card, similar to the bomb threat checklist required to be maintained near telephones. The Network Emergency Response card provides a description of symptoms to watch for and report; it also includes recommended response actions.

The Joint Task Force – Computer Network Defense (JTF-CND) is a subordinate Command of USSPACECOM and is located in Washington, D.C. With the realignment of the JTF-CND under USSPACECOM, it was able to launch efforts to protect and defend information vital to the nation’s military forces and defense agencies. DoD is increasing its IA capability and bolstering local CND of all networks operated as part of the Defense Information Infrastructure. The scope of CND is global in nature, looking across all DoD networks to ensure that no malicious activity goes undetected. While this vital mission area is highly technical and embryonic, JTF-CND is committed to success. USSPACECOM’s top CND priorities include obtaining the resources necessary to successfully execute the mission; conducting real-world operations and support; planning and conducting a major joint CND exercise; and addressing a wide range of policy, doctrine, and requirements associated with global CND. Although the JTF-CND has garnered several successes recently, including the Y2K rollover, the mission does not allow them to rest on their laurels.

N-SP J6 is engaged in an ongoing effort to map all the NIPRNET and SIPRNET networks that impact the NORAD and USSPACECOM missions. This includes all networks on all bases and installations that have a NORAD and/or USSPACECOM unit or supporting sensor located there. The network map will identify all the critical servers and the applications running on them.



An ANTCS-85B communications van under camoflauge monitors area communications in Hungary.

Within the last decade, communications systems have undergone a major transformation as the concept of a global shared data network has reinvented the way that service is provided to the customer. Communicators are beginning to recognize that increased bandwidth does not necessarily provide increased performance. The factors involved in providing guaranteed information flow have grown beyond calculations of the "busy hour" and are now expressed in terms of end-to-end parameters such as latency, throughput, and availability.

As more and more bandwidth-intensive and mission-critical applications are introduced into NORAD’s SIPRNET and RELCAN network, serious consideration should be given to determining whether current network design and configuration can support these applications.

The overall objective of the November 1999 IA Conference was to educate NORAD-USSPACECOM Headquarters and Component staffs on the direction of the Chief Information Officer (CIO) IA Initiative. It also sought to determine the status and direction of the NORAD-USSPACECOM computer and staff resources with regard to Security Policies; Network Architectures; IA Concept of Operations (CONOPS) Development; IA Training and Education Requirements; and IA Risk Assessments.

The IA mission as stated at the Conference is to defend NORAD-USSPACECOM information and information systems against intentional, unintentional, and natural threats; to provide IA situation awareness to the CINC; and to direct NORAD-USSPACECOM's IA program through effective policy, processes, and practices.

The INFOCON Conference of 13–15 June 2000 was very successful. One area it covered was the current DoD INFOCON process and the operational impacts associated with INFOCON implementation from a C/S/A perspective. In concert with this, it sought to discuss operational criteria to declare appropriate INFOCON levels, it reviewed the proposed framework for new DoD INFOCON levels, and it developed directive actions for each INFOCON level.

The relatively new concept of Network Centric Warfare (NCW), defined as having a robust, interconnected network of sensor-to-shooter information flow, is what NORAD and USSPACECOM are seeking to expand and improve in order to achieve Information Superiority in future operations. This NCW concept is at the heart of the IA CONOPS. USSPACECOM strongly advocates the design of more open and interconnected networks of sensors, correlation, and operations centers over some of today's current network architectures composed of individual stove-piped systems.

U.S. SOUTHERN COMMAND

The U.S. Southern Command (USSOUTHCOM) is headquartered in Miami, Florida. USSOUTHCOM's Area of Responsibility (AOR) includes all of Latin America south of Mexico, including the Caribbean. Its stated mission is to shape the environment within its AOR by conducting military-to-military engagement and counterdrug activities to help promote democracy and stability and hinder threats to regional security. To accomplish its mission, USSOUTHCOM depends on the protection and availability of its information and information systems. USSOUTHCOM's Information Assurance (IA) program implements the Defense in Depth (DiD) concept by continuously training its people on information security, improving its network defense operations, and integrating effective systems by monitoring technology throughout the AOR.

Over the past fiscal year, the Command has significantly increased its use of Information Operations (IO) and IA. The Command expanded programs that had been implemented and proven successful at its Headquarters to its Security Assistance Organizations (SAOs) and Direct Reporting Units (DRUs). Emphasis was placed on expanding their IA capabilities from securing only data networks to securing voice and video networks as well. All three types of information are equally important and equally potentially vulnerable.

Through the continued operation of its Information Technology Management Board (ITMB), USSOUTHCOM continues to increase IA visibility of all networks at all levels. The Architecture and Engineering and Process Improvement Working Groups and the Configuration Management Working Group (CMWG) combine to provide the ITMB with a structure for decision support. This ensures that USSOUTHCOM operators can rely on the information they need to perform their missions. With the relative explosion of information systems technology and USSOUTHCOM's move from Panama to Miami, Florida, three years ago, it became imperative for the Command to develop a centralized view of its Command, Control, Computers, and Communications (C4) systems. The CMWG was created to pull together all the pieces of the Command's C4 structure and present a Command-level baseline. By using this baseline as a starting point for all C4 system modifications, USSOUTHCOM will be able to prevent known vulnerabilities from reoccurring and ensure that each new or modified system conforms to IA standards.

The future of IA at USSOUTHCOM will continue to include security awareness, training, and education (SATE), operationalizing IA, theater systems configuration management, and continued assessments of its network defense posture. Continuing these three efforts will ensure the best possible protection to critical information and critical information systems.

USSOUTHCOM has approached IA very seriously and taken many important steps in establishing and maintaining a robust IA posture. The USSOUTHCOM IA Division completed IA assessments and certification and accreditation (C&A) packages for 14 countries within its AOR. These assessments will help ensure that permanent and temporarily deployed personnel throughout the AOR can operate under most threat conditions. Connectivity and security challenges have become more difficult because of USSOUTHCOM's significant expansion of the SIPRNET and NIPRNET to many of the units and teams operating in areas where there exist a high probability of natural disaster and low availability of local infrastructure services.

USSOUTHCOM has also taken an active role in assessing its own IA posture through the exercise "Blue Advance 99," which highlighted the vulnerabilities of nonsecure voice through COMSEC monitoring. With this in mind, a renewed Command emphasis on improved OPSEC and COMSEC practices was clearly evident during the next exercise, "Winter Picnic 99." Also, the increased demand for secure voice resulted in the purchase of more than 200 Secure Terminal Equipment (STE) telephones and an agreement for USSOUTHCOM to be the testbed for the new STEs.

A surveillance operator at the Southern Regional Operations Center looks for drug traffickers in the air on his radar scope.

By standing up the Command's Theater Network Coordination Center (TNCC), USSOUTHCOM emphasized improved network monitoring, management, and administration. Along with that effort, the Command installed the new Joint Defense Information Infrastructure Control System-Deployed (JDIICS-D) network monitoring equipment at USSOUTHCOM Headquarters and two other key locations. The three monitors were integrated through the use of a Virtual Private Network and they provided a theaterwide view of the Command's data network performance. In addition, USSOUTHCOM updated Command Information Operations Condition (INFOCON) processes. It conducted a joint DISA/USSOUTHCOM tabletop IA exercise

(NADIR NOVA) to refine the Request for Information (RFI) process, INFOCON implementation/reporting, and Command staff relationships.

To maintain the most up-to-date IA information, USSOUTHCOM aggressively updated the Information Assurance Vulnerability Alerts/Bulletins (IAVA/Bs) and Technical Advisories reporting and compliance process. It developed a plan to transition from the manual reporting method to the Vulnerability Compliance Tracking System. USSOUTHCOM also continued to reinforce user awareness training through the monthly publication of The Informer, the Command's IA bulletin. This publication highlights and disseminates information on noteworthy issues such as INFOSEC training, password guidelines, computer hacker threats, STU-III rekey procedures, and individual Internet user responsibilities. The Informer is also published on the Command's website and continues to receive positive reviews. Finally, USSOUTHCOM continuously modernized its security awareness training and education, as well as its certification programs. The Command tracked and assisted in the certification of more than 240 information systems security professionals, including more than 200 systems administrators through Level I certification.

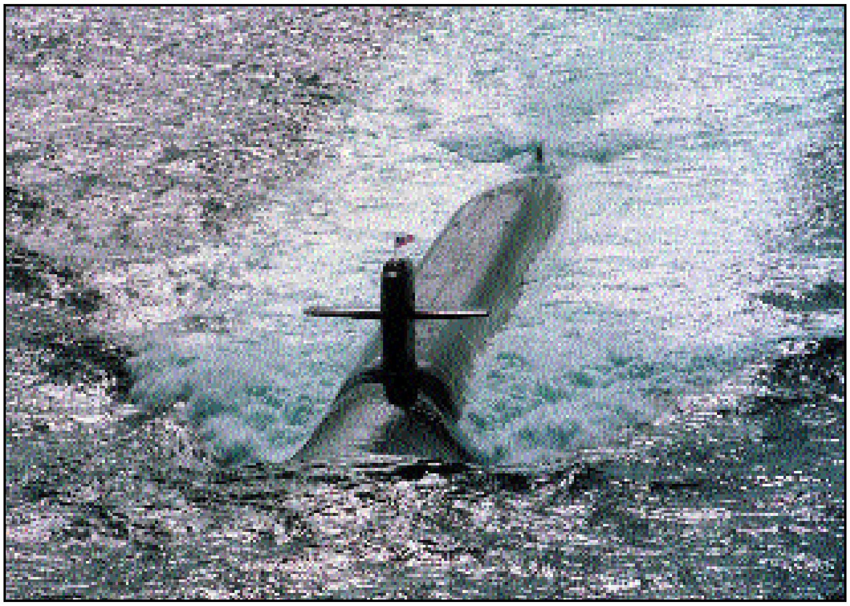
U.S. STRATEGIC COMMAND

United States Strategic Command (USSTRATCOM), headquartered at Offut AFB, Nebraska, is responsible for defending the United States through the strength of the deterrence of the nation's strategic forces. These forces comprise the strategic triad of nuclear weaponry-fleet ballistic submarines, intercontinental ballistic missiles (ICBMs), and long-range strategic bombers.

Making IA a Daily Concern

USSTRATCOM has consistently demonstrated strong commitment to establishing a leading-edge IA program. The program is built on a foundation of cooperation and partnership at the national and local levels, integrating the capabilities of people, technology, and operations. USSTRATCOM IA leaders have inculcated Information Security (INFOSEC) such that all Command personnel from the most-junior enlisted personnel to Flag Officers "walk the point" daily and regularly alert security staff to any unusual events. Likewise, the Command has ensured that IA was built into all operational and contingency plans. This strong commitment has undoubtedly helped strengthen national security.

USSTRATCOM has developed an aggressive and successful training program. Through specialized web-based training, personnel from routine users to systems administrators are given timely, relevant information in a variety of current security topics. As a result, Command personnel realize the critical nature of security and take personal responsibility for adhering to sound security polices and procedures. Junior enlisted personnel have frequently detected warnings on worldwide malicious code events



A Fleet Ballistic Missile Submarine armed with Trident missiles cruises on the surface.

and raised the alarm. In addition, USSTRATCOM general officers were the first to discover the "Melissa" virus and later the "ILOVEYOU" virus/worm.

USSTRATCOM's Information Operations Support Staff (IOSS) is the cornerstone of the Command's IA program. The IOSS was established to provide an overarching view of the Command's information-processing infrastructure. This cross-functional team comprises representatives from the Information Operations Division, Plans Directorate, Intelligence Directorate, Information Technology Support Division, DISA Field Service Office, Public Affairs Branch, Legal Branch, and other Intelligence Community representatives. The IOSS has been instrumental in protecting the Command's command, control, communications, and computer systems by establishing information protection processes, security infrastructures, and systems integration.

USSTRATCOM has established its own Computer Emergency Response Team (STRATCERT) and is in collaboration with the Omaha cybercommunity and Offutt AFB to protect computer networks. Through reconfiguration of USSTRATCOM's external router, the electronic traffic load on the firewall was reduced by 70 percent. This allowed STRATCERT to focus more of its resources on identifying suspicious activity within its enclave. As an example, STRATCERT identified inappropriate local traffic originating from an Omaha nonprofit organization (NPO) and worked with the NPO network administrators to identify the source, eliminate it, and make both networks more efficient.

IA Awareness

To ensure that the Command's IA Community stays abreast of ongoing network security initiatives, the Command IA officer created the IA Working Group. The roles, relationships, and responsibilities defined by this group enabled the Command to respond to, and recover from, the "ILOVEYOU" virus with no mission impact. Deliberate preplanning allowed customers to continue using network services while the Command was isolated pending countermeasures. As a result of this incident, the working group took proactive action to prepare for similar events in the future. When the "stages" worm hit several months later, there was no impact to USSTRATCOM, even though many sites worldwide experienced serious disruptions.

USSTRATCOM partnered with industry to establish the Omaha InfraGard Chapter in support of Presidential Decision Directive (PDD) 63. The National Infrastructure Protection Center (NIPC) now ranks this chapter among the top three in the nation. It serves as the focal point for private- and public-sector representatives to spearhead computer security issues and share common computer security threats and vulnerabilities. Interest in Omaha's chapter inspired subchapters in Des

Moines, Iowa, and Milwaukee, Wisconsin. USSTRATCOM's leadership motivated the NIPC to enhance information sharing for InfraGard members nationwide.

USSTRATCOM conceived, led, and administered the Omaha Cyber Security Conference in May 1999. This event led to a volunteer effort to increase IA awareness in Omaha. The Cyber Security Forum was established after the conference to share information among interested individuals and companies. More than 30 participants regularly attend these meetings, where information security topics are discussed and best practices shared. As a result, several local firms have adopted e-mail content scanners to assist in protecting their networks.

USSTRATCOM formed an important partnership with the Peter Kiewit Institute of Information Science, Technology, and Engineering. The Institute is a merger of the University of Nebraska at Omaha's College of Information Science and Technology and the University of Nebraska at Lincoln's College of Engineering and Technology. The collaborative partnership was formed to meet the ever-increasing need for IT professionals in the Omaha area and around the nation. USSTRATCOM partnered with the Institute to develop a "Cybersecurity" curriculum comprising five to six courses for a specialized certification program in information security. Area business representatives have endorsed this program. Realizing the importance of first-hand cybersecurity experience, more than 20 of USSTRATCOM's IT professionals volunteered their time to personally mentor university students. USSTRATCOM believes that this program will satisfy a vital need to attract top students to local and national infrastructure protection efforts. USSTRATCOM's workforce has benefited from this program by hiring six students as interns. USSTRATCOM contractors have hired an additional 10 students. The Institute's goal is to become an NSA-recognized "Center of Excellence."

Strengthening IA Through Practice

USSTRATCOM maintains a very robust Communications Security (COMSEC) monitoring program. During the annual exercise, GLOBAL GUARDIAN, monitoring efforts included various aspects of the entire strategic triad, including ICBMs, bombers, and submarines. Monitoring of command-and-control (C2) systems included telephones, pagers, facsimile machines, high frequency, ultra high frequency, and computer-to-computer. The Command's successful COMSEC program stems from its in-house initiatives: adoption of an electronic key management system, an aggressive secure telephone equipment (STE) acquisitions program (more than 100 on-hand to date), and a semiannual awareness notification reminder letter sent to all USSTRATCOM users. As a result, metrics from the past three years indicate a 60 percent decrease in USSTRATCOM COMSEC violations and related disclosures of "essential elements of friendly information."

Command efforts to ensure IA by leveraging operations security (OPSEC) practices were highly successful. Based on lessons learned from Command exercises, the OPSEC working group is broadening the scope of OPSEC awareness and training to include all assigned forces. This first-ever "traveling OPSEC road show" will visit each USSTRATCOM Task Force (TF) to provide lessons learned and awareness training to ensure compliance. In addition, the Command recently reinforced its OPSEC policies by requiring shredding of any paper/text products generated by Command personnel. Regular inspection of trash receptacles ensures compliance. Any office paper found is investigated to determine its source.

The B-52 Stratofortress fulfills the mission of long-range heavy bomber.

USSTRATCOM approached NSA and DISA to assess the security posture of its subordinate Command locations and to ensure that they have access to the most current computer security assessment tools and techniques available. USSTRATCOM initiated a program with NSA and DISA to expand its Command IA Operations Reviews to include the TFs. The set of outside eyes from NSA, DISA, and USSTRATCOM personnel allowed USSTRATCOM to thoroughly address, assess, and enhance the IA programs at its TFs.

In 1997, USSTRATCOM recognized the need to rapidly heighten awareness and technical safeguards against a cyberattack. As a result, it developed the Information Operations Conditions concept, which is similar to the Defense Condition (DEFCON) system. This year, USSTRATCOM is spearheading an effort to further standardize and streamline the flow of information during a cyberattack by advocating the use of the strategic warfare voice conference systems. This will enable rapid DoD-wide dissemination of any Defense Information Infrastructure attack warning and recommendations for immediate IA response by the Joint Task Force – Computer Network Defense (JTF-CND). DoD-wide implementation of this proposal will greatly enhance the ability to rapidly respond to cyberattack. In addition, USSTRATCOM is the leading advocate for ensuring standardization of these Information Operations Conditions (INFOCONs) across DoD so that a directed posture results in DoD-wide consistent action.

European Command (USEUCOM) requested and received imagery intelligence support from USSTRATCOM during Operation ALLIED FORCE. During analysis, these mission-critical files were kept safe, and the confidentiality and integrity of battle damage assessment and poststrike retargeting information were assured by USSTRATCOM's combination of physical security, host system security, electronic perimeter defense, and intrusion detection systems.

Making Use of IA Technologies

USSTRATCOM recognizes the need for a robust suite of tools to detect attacks and protect the Command's information and information systems. As part of an overall campaign, USSTRATCOM continuously surveys and tests the latest cutting-edge tools from industry in order to stay ahead of any potential adversaries.

USSTRATCOM personnel continue to research and integrate technologies to increase and enhance the protection of our information systems. In 1999, USSTRATCOM implemented a COTS software security tool to monitor and control all incoming e-mail traffic. This product uses a Command-determined set of expression-based rules, which gives to administrators an automated method that allows them to detect potential hostile code and filter inappropriate content, thus preventing it from entering into the Command's information infrastructure. Specifically, during the "ILOVEYOU" virus attack, STRATCERT expanded on proven tactics and techniques perfected during the "Melissa" virus outbreak to assist the COTS product vendor in developing critical product modifications. These modifications allowed STRATCERT to institute malicious code protection measures ahead of the antivirus vendors. More than 5,000 "ILOVEYOU" viruses and variants were repelled before they could impact mission.

USSTRATCOM is leading the way in a major DoD pilot project to replace or augment the Joint Intrusion Detection System with a COTS automated, real-time intrusion response system. This leading-edge product expands the Command's already robust suite of detection tools, ensuring immediate around-the-clock intrusion detection notification. It unobtrusively analyzes activity across both the Unclassified and Secret Command networks and alerts operators to potential attacks. Lessons learned will be shared by all Unified Commands.

USSTRATCOM is continuing to explore new territory in another major DoD pilot project as the first Command to install the Intrusion and Misuse Deterrence System (IMDS) on a Secret network. These data will provide STRATCERT analysts with a keener sense of potential attack methodologies and assist local and national decision makers in enhancing network security policy and guidance.

USSTRATCOM is the DoD Operational Manager for the Advanced Concept Technology Demonstration (ACTD) to develop an Automated Intrusion Detection Environment (AIDE). STRATCERT identified the need for an early-warning cyberattack detection system and successfully tested this combined sensor fusion system at STRATCERT this year. Knowledge gained from technical research and annual operational demonstrations is being leveraged into ongoing DoD IA initiatives and implemented into actionable tactics, techniques, and procedures. As an example of the unique usefulness this system delivers, AIDE correlated a series of "stealthy" events and alerted STRATCERT to a potentially serious real-world attempt to prepare the cyberbattle space. Data correlated from several remote detection sources triggered the report of a potential "Firewalker" exploit in progress—one of the first coordinated events of its kind. This robust capability will be the first ever to create a "global" integrated intrusion detection system.

A Trident II nuclear capable missile breaks the surface of the water after being launched by a submerged Fleet Ballistic Missile Submarine.

USSTRATCOM's IA program is built on a foundation of cooperation and partnership, integrating the capabilities of people, technology, and operations to establish a multidimensional program. Senior leadership involvement and commitment to IA ensure that the Command integrates IA into real-world operations and planning. Through continued partnership with local private and public communities, USSTRATCOM has become a model for PDD 63 implementation. All efforts combined make IA truly operational at USSTRATCOM. In November 2000, NSA recognized USSTRATCOM's successful IA program as NSA's 1999 Rowlett Award winner for organizational excellence in IA.

U.S. TRANSPOR TATION COMMAND

The United States Transportation Command (USTRANSCOM) is headquartered at Scott AFB, Illinois. USTRANSCOM is responsible for providing air, land, and sea transportation for the DoD in times of peace and war. USTRANSCOM conducts this mission through the management of the Defense Transportation System (DTS)—the people, equipment, and systems that move DoD personnel and materiel around the world.

USTRANSCOM's Information Systems Security Branch is responsible for securing the global transportation network by enforcing its Information Systems Security Program around the clock. It is currently manned by 3 military, 2 GS civilians, and 18 contractor personnel. USTRANSCOM pursues a proactive and aggressive approach to implementing and maintaining its award-winning IA posture.

Currently, much of USTRANSCOM's logistics mission is accomplished through private-sector commercial partnerships, with transactions conducted almost exclusively through the World Wide Web. As a result, Unclassified USTRANSCOM systems are open to attack from worldwide hackers with varied skill levels and resources. Therefore, the need to protect sensitive DoD information in this potentially hostile Internet environment is vitally important in supporting the USTRANSCOM mission. USTRANSCOM's security program protects its data by incorporating a tactical redundancy that replicates Unclassified transportation information as it migrates from the NIPRNET to the SIPRNET through one-way, high-speed command-and-control guards.

In FY 2000, USTRANSCOM drafted an Information Operations Conditions (INFOCON) Policy Directive that identifies the technical measures required to achieve each INFOCON level. Also authored was a policy directive for network incident reporting. USTRANSCOM ensured that it corresponded to the operational reporting procedures and requirements levied by the NSA and DISA.

USTRANSCOM developed an IA appendix to the USTRANSCOM Joint Military Readiness Review (JMRR) process that identified a methodology for determining combat readiness (C-ratings) for the IA graded area. As the result of USTRANSCOM's efforts, a successful system was developed that combined USTRANSCOM baseline analysis results, Joint Staff IA metrics, and weighting criteria across operational parameters to objectively evaluate IA functions.

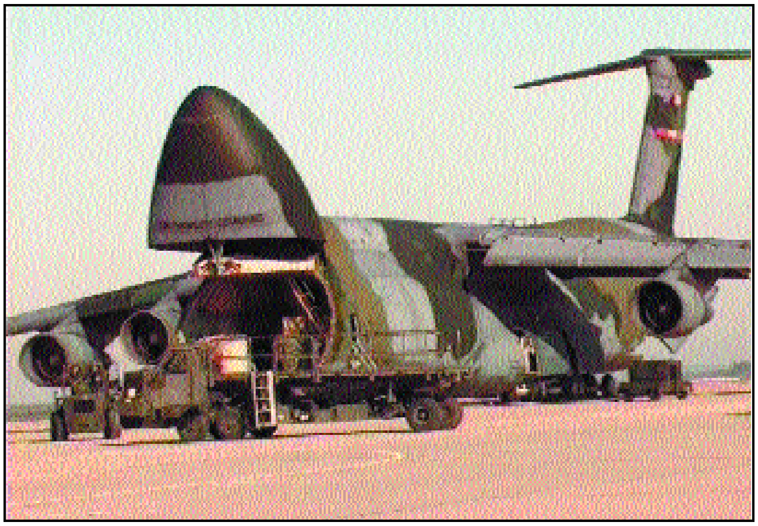
Information Security Exercises

In 1999, USTRANSCOM executed its first-ever dedicated INFOSEC exercise. The highly successful tabletop exercise known as Paradise Express (PE-I) involved the entire Scott AFB community in two days of intense information operations war-gaming. It was followed by

Paradise Express II (PE-II), which built upon the lessons learned from PE-I. PE-II involved the Transportation Component Commands (TCCs) and used GOTS Logbook software to automate the incident reporting process. Early in 2000, the series was capped by the Paradise Express III (PE-III) exercise, which was executed in conjunction with another USTRANSCOM capstone exercise, Turbo Challenge 2000. As the result of these enhanced Paradise Express training exercises, security personnel validated existing tactics, techniques, policies, and procedures for protecting USTRANSCOM assets.

Integration Activities

USTRANSCOM is integrating its Headquarters security infrastructure with the Service Component Commands through an intense Information Assurance/Information Protection (IA/IP) program. IA/IP provides the Components' computer security personnel with advanced security tools. It also gives them access to the expert engineering guidance and resources of Headquarters. Making these capabilities available to Component security staff has helped improve Component security personnel proficiency. The USTRANSCOM IA/IP program also provides visual display of the configuration, health, and status of the entire DTS information architecture, monitored by its Global C4 Coordination Center (GCCC). The GCCC will provide to USTRANSCOM key decision makers a vital tool for assessing the operational security of command and control systems.



A C-5 unloading stores.

IA Panel Participation

USTRANSCOM is integrating the DoD's KMI/PKI initiative through the testing of the "Single Sign-On" capability. When operational, this initiative will give users the ability to access authorized applications by using DoD PKI-authenticated certificates.

During Y2K, USTRANSCOM produced a USTRANSCOM NT Security Handbook that was derived from NSA, DISA, Air Force, Navy, and other NT Configuration resources. USTRANSCOM also has established a relationship with the NSA ISSO Work Group and participated in the NSA effort to produce a Microsoft Windows 2000 Security Configuration Guide. USTRANSCOM's proven model for policy-based intrusion detection has been featured in technical periodicals and has been a topic of lectures presented at the prestigious Washington University in St. Louis, Missouri.

USTRANSCOM continues to be a major contributor to the DoD IA Panel as it develops the DoD policy for mobile executable code. In addition, USTRANSCOM's mobile code policy was a baseline resource used in developing the Panel's mobile code policy document for DoD.

USTRANSCOM actively manages the USTRANSCOM Secret and Below Interoperability (SABI) process. In FY 2000, the Command helped bring the Global Transportation Network (GTN) system into full SABI compliance. In addition, DITSCAP doctrine is incorporated in the development and maintenance of all USTRANSCOM major information systems.

Glossary

Availability
Timely, reliable access to data and services for authorized users.

C^{3}I
Command, Control, Communications and Intelligence (C3I). Functions include information policy and information management, command and control, communications, counterintelligence, security, information assurance, information operations, space systems and space policy, intelligence, surveillance and reconnaissance, and intelligence-related activities conducted by the Department.

Computer Emergency Response Team (CERT)
A cadre of IT professionals whose responsibility is to protect, defend, and restore the integrity and availability of the essential elements and applications of their organization’s networks and on a larger scope the Defense Information Infrastructure. DISA fields the DoD CERT that has overall responsibility for the integrity of DoD networks however, most DoD activities maintain some version of a CERT to address their specific needs.

Confidentiality
Assurance that information is not disclosed to unauthorized persons.

Commercial-off-the-Shelf (COTS)
Equipment and software which is purchased from vendors, as manufactured, without modification, for use in government systems.

Congressional Justification Book (CJB)

Documents plans for expenditures within the president’s Budget and provides validation for it. CJBs are prepared by Components and submitted to Congress for each fiscal year.

Critical Infrastructure Protection (CIP)

The portion of telecommunications electrical power systems banking and finance, transportation, water supply and emergency services which comprise critical infrastructures from physical and cyber threats.

Critical Success Indicator (CSI)

Standards that correlate to the highest levels of IA metrics and which are used to determine Readiness measures of success.

Common Access Card (CAC)

A common access card is a credit card-sized device that contains one or more integrated circuit chips, and may also have additional technologies such as: a magnetic stripe, bar codes, radio frequency transmitter, and photo identification. The Uniformed services are working with the DoD to bring smart card technology to all of its members. The CAC will have several functions – literally combining several cards into one. In addition to replacing the existing DoD identification card, it will be the:

- Principal card used to enable physical access to buildings and controlled spaces;
- Principal card used to enable computer network and system access; and
- Primary platform for the Public Key Infrastructure (PKI) token.

Defense in Depth (DiD)

The strategy that DoD is pursuing to ensure success in all types of warfare that are dependent on information superiority. The notional view of Defense in Depth is analogous to a medieval castle and the various layers of protection that surround it. e.g., walls moats, and drawbridges.

Defense Information Infrastructure (DII)

The Defense Information Infrastructure facilitates linking joint command organizations to the military service command and control systems as an integral part of achieving information dominance. From a network and systems management perspective, the DII is composed of three "blocks" or domains: the sustaining base block (managed locally by CINC/service/agency control), the long-haul block (managed by the Defense Information Systems Agency), and the deployed block (managed by the joint task force commander).

Defense Information System Network (DISN)

DISN is the subset of the Defense Information Infrastructure, primarily providing information transport services both within the Defense Information Infrastructure and across the Defense Information Infrastructure boundaries. The Defense Information Infrastructure is a seamless web of communications networks, computers, software, databases, applications, and other capabilities that meets the information processing and transport needs of DoD users in peace and in all crises, conflict, humanitarian support, and wartime roles.

Defense-wide Information Assurance Program (DIAP)

The Defense-wide Information Assurance Program (DIAP) was established by DoD to provide a common management framework and central oversight to protect the Defense Information Infrastructure, or DII.

DoD Information Technology Security and Certification and Accreditation Process (DITSCAP)

DITSCAP defines a process that standardizes all activities leading to a successful certification and/or accreditation. The primary purpose of the process is to protect and secure the elements that comprise the Defense Information Infrastructure, regardless of owner service or agency. By standardizing the process, the risks attendant to non-standard security implementation across shared infrastructure and end systems are minimized. DITSCAP incorporates a formal, four-phased approach to certification and accreditation: Definition Phase, Verification Phase, Validation Phase and Post-Accreditation Phase.

Enclave

A computing environment that is under the control of a single authority with personnel and physical security measures; may control multiple networks.

Firewall

A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one, which exists to block traffic, and the other, which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic.

Functional Evaluation and Integration Team (FEIT)

One of the two teams within DIAP, the Functional Evaluation and Integration Team (FEIT) continuously evaluates DoD component and IA programs to ensure that the defense-wide application of IA functions is consistent, integrated, efficient, and programmatically supported.

Global Information Grid (GIG)

The Global Information Grid is a globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information, on demand, to warfighters, policy makers, and support personnel.

Global Information Infrastructure (GII)

The GII is a worldwide assembly of systems that integrates five essential components:

- communications networks, such as telephone, cellular, cable and satellite networks;
- information equipment/appliances, including computers, televisions and telephones;
- information resources, including educational materials, medical databases, and entertainment and commercial programs;
- applications, such as telemedicine, electronic commerce and digital libraries; and
- people of all skill levels and backgrounds.

The GII will continually evolve as it incorporates more advanced technologies, new information, new consumers and different ways to use its resources.

Joint Task Force-Computer Network Defense (JTF-CND)

The JTF-CND will serve as the focal point with the DoD efforts directed at defending computer networks and systems. CND involves monitoring incidents and potential threats to DoD systems and establishes links with other federal agencies through the National Infrastructure Protection Center to share information on activities across the information infrastructure. When attacks are detected, recovery actions are undertaken to stop or contain damage and restore network functions to DoD operations.

Information Assurance Vulnerability Alert (IAVA)

A program managed by DISA through its DoD Computer Emergency Response Team component which incorporates the identification and evaluation of new computer network vulnerabilities, disseminates technical responses through both message traffic and web site postings, and tracks compliance within the DoD community.

Identification and Authentication (I&A)

A process used by a system to recognize an entity. A security measure designed to establish the validity of a transmission, message or originator, or as a means of verifying an individual's authorization to receive specific categories of information with some degree of assurance.

ILOVEYOU virus

A widely distributed VBScript worm with virus qualities that was maliciously spread in May 2000. Its most common tactic was utilizing a host's Microsoft Outlook to spread itself to all other addresses in the host address book. Once executed, it replaced, modified and deleted various files on the host computer.

Information Assurance (IA)

Information Assurance (IA) represents measures to protect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems. IA is accomplished by applying end-to-end security measures to the information we process and the systems we use to process that information. This is done by integrating and practicing communications security (COMSEC), computer security (COMPUSEC), emission security (EMSEC), and security awareness, training, and education (SATE). The result is information for missions that is available, accurate, and secure.

Integrity

Protection against unauthorized modification or destruction of information.

Internet

The Internet is a vast network of networks spanning over 170 countries in the world. It links computers of many different types, sizes, and operating systems, and, of course, the many people of those countries that use the Internet to communicate.

Intranet

An Intranet applies Internet technologies and applications to a closed networks within an organization (or company) to achieve better results than the more conventional means of data access and transfer. Intranets helps in cutting costs, and provides easy and fast accessibility of day to day information.

Intrusion Detection System (IDS)

May run either on the target machine who watches its own traffic (usually integrated with the stack and services themselves), or on an independent machine watching all network traffic (hub, router, probe). It monitors packets on the network wire and attempts to discover if a hacker/cracker is attempting to break into a system (or cause a denial of service attack).

Joint Vision 2020 (JV2020)

Joint Vision 2020 is a JCS doctrine that builds upon and extends the conceptual template established by Joint Vision 2010 to guide the continuing transformation of America's Armed Forces. The overall goal of the transformation described in this document is the creation of a force that is dominant across the full spectrum of military operations – persuasive in peace, decisive in war, preeminent in any form of conflict.

Key Management Infrastructure (KMI)

A secure and trusted system for generation, storage, distribution, account and control of cryptographic keys.

Melissa Virus

The Melissa virus was a macro virus, which spread from user-to-user via infected MS-Word files. It was first uploaded to certain Internet Newsgroups from an AOL account, and has spread worldwide. It was designed to be fast spreading, by exploiting a user's e-mail program to send itself automatically to others and used Microsoft Outlook to spread by sending infected Word documents as attachments to the top fifty addresses in a user's Outlook Global Address Book. This virus was first detected in March 1999.

National Information Infrastructure (NII)

The modern National Information Infrastructure (NII), sometimes called the "information superhighway," is an interconnection of computers and telecommunication networks, services and applications.

NetOps

An organizational and procedural framework intended to provide information systems and computer network owners the means to manage their information systems and computer networks in order to effectively execute their mission priorities.

NIPRNET

Unclassified but sensitive Internet Protocol Network, one of two types of Internet Protocol routers owned by the Defense Information System Network.

Nonrepudiation

Assurance that data being sent is provided with proof of delivery and that the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data.

People

People, using technologies to conduct operations, are a central element of Defense in Depth. In this context, the term people refers to personnel who design, build, install operate, assess, evaluate and maintain protective mechanisms.

Program Development and Integration Team (PDIT)

One of the two teams within DIAP, the Program Development and Integration Team (PDIT) provides for the oversight, coordination and integration of DoD IA resource programs.

Public Key Enabling (PKE)

The enabling of information system applications to utilize the services of a pubic key infrastructure. This includes activities and resources associated with the cost of manpower, hardware, software, encryption services, and support efforts needed to make applications capable of employing digital certificates and signatures.

PKI Registration Authority

Authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Public Key Infrastructure (PKI)

Public-key infrastructure (PKI) is the combination of software, encryption technologies, and services that enable enterprises to protect the security of their communications and business transactions on the Internet. A public-key infrastructure (PKI) enables an enterprise to provide authentication, access control, confidentiality, and non-repudiation for its networked applications using advanced technologies including digital signatures, encryption, and digital certificates.

SIPRNET

Secret Internet Protocol Router Network (SIPRNET), one of two types of Internet Protocol routers owned by the Defense Information System Network.

Virtual Private Network (VPN)

Usually refers to a network in which some of the parts are connected using the public Internet, but the data sent across the Internet is encrypted, so the entire network is "virtually" private. A typical example would be a company network where there are two offices in different cities. Using the Internet the two offices merge their networks into one network, but encrypt traffic that uses the Internet link.